SOLVING THE DILEMMA OF STATE RESPONSES TO CYBERATTACKS: A JUSTIFICATION FOR THE USE OF ACTIVE DEFENSES AGAINST STATES WHO NEGLECT THEIR DUTY TO PREVENT

LIEUTENANT MATTHEW J. SKLEROV[*]

[*] Judge Advocate, United States Navy. Presently assigned as Student, 57th Judge Advocate Officer Graduate Course, The Judge Advocate General's School, United States Army, Charlottesville, Virginia. J.D., 2002, The University of Texas School of Law; B.A., 1997, State University of New York at Binghamton (*cum laude*); A.A., 1995, State University of New York at Rockland. Previous assignments include Deputy Command Judge Advocate, USS NIMITZ (CVN 68), 2006-2008; Command Judge Advocate, Naval Air Station, Kingsville, Texas, 2004-2006; Trial Counsel, Trial Service Office West, Detachment Bremerton, Washington, 2003-2004. Member of the bars of Texas, the U.S. District Court for the Southern District of Texas, the U.S. Court of Appeals for the Armed Forces, and the U.S. Supreme Court. This article was submitted in partial completion of the Master of Laws requirements of the 57th Judge Advocate Officer Graduate Course. The author would like to thank Major J. Jeremy Marsh, U.S. Air Force, for his invaluable assistance with this article.

Table of Contents

> *How do you account for your discoveries? Through intuition or inspiration?*[1]
>
> *Both. . . . I'm enough of an artist to draw freely on my imagination, which I think is more important than knowledge. Knowledge is limited, imagination encircles the world.*[2]

I. Introduction

The greatest advances in law, like those in science, come through imagination. When scientific knowledge fails to explain new discoveries about the universe, scientists advance new theories to account for their discoveries—so too with the law. Revolutions in technology, like the internet, challenge the framework that regulates international armed conflict.[3] Legal scholars must use imagination to find ways to tackle this problem. If not, the law will become obsolete and meaningless to the states that need its guidance.

Man has long sought to regulate warfare. From the Chivalric Code to the U.N. Charter, man has placed restraints on the times one can resort to war and the methods with which it's conducted. There are a variety of reasons why, but, to generalize, regulations are the response to perceived problems with the state of war at a given time. Sometimes these perceptions are the result of shifts in the social conscience. At other times, values haven't changed at all, but problems arise due to radical changes in the way war is waged.

Needless to say, as warfare changes, so must the law; and warfare is changing fast. Traditionally, the instruments of war were only controlled by states. However in today's

[1] George Sylvester Viereck, *What Life Means to Einstein: An Interview by George Sylvester Viereck*, PHILA. SATURDAY EVENING POST, Oct. 29, 1929, at 113 (questioning Albert Einstein about his discoveries).

[2] *Id.* at 117 (quoting Albert Einstein's response to his questions).

[3] Michael Schmitt, *Bellum Americanum: The U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict*, 19 MICH. J. INT'L L. 1051, 1058–59 (1998).

world of globally interconnected computer systems, non-state actors with a laptop computer and an internet connection can attack the critical infrastructure[4] of another state from across the world. This is a major paradigm shift, which the law of war fails to adequately address.

Cyberattacks[5] pose unique challenges to the law of war, especially when conducted by non-state actors. New interpretations of the law of war are needed to deal with these challenges. This paper will explore these challenges and provide an analytical framework for dealing with them. Once the current state of international law regarding the use of force is fully explored, this paper will demonstrate its author's conclusions that states have a right under international law to: (1) view and respond to cyberattacks as acts of war and not solely as criminal matters, and (2) use active, and not just passive, defenses against other states who may or may not have initiated an attack, but have neglected their duty to prevent cyberattacks from within their borders.

These conclusions will be demonstrated over the seven parts of this paper. Part I introduces the legal problems states encounter when dealing with international cyberattacks. It explains why current interpretations of the law of war limit states from using active computer defenses against cyberattacks, and explains why this restriction endangers states. It questions the validity of current interpretations of the law of war, and lays the foundation for the rest of the paper. Part II provides background information on cyberattack methods,

[4] "Critical infrastructure are those systems, physical or virtual, whose incapacitation or destruction would have a debilitating impact on the nation's security, economy, public health or public safety." Critical Infrastructure Protection Act of 2001, 42 U.S.C.S. § 5195c (2001).

[5] This paper uses derivatives of the root word cyber, such as cyberattack, cyberthreat and cyberwarfare. Cyber may be used as an adjective or combining form that when used in connection with other words, defines them as relating to computers or computer networks. So, a cyberattack would be an attack carried out against a computer or computer network; a cyberthreat would be a threat to a computer or computer network. Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/cyber (last visited Mar. 22, 2009).

capabilities and defenses. Part III lays out the basic framework for analyzing armed attacks. Part IV explores the challenges that armed attacks by non-state actors present to the basic framework of the law of war, and explains the limits on state responses to them. Part V analyzes cyberattacks under the law of war. It demonstrates that some cyberattacks are armed attacks, that states have a duty to prevent cyberattacks, and that states have a right to use active defenses against states that neglect their duty to prevent cyberattacks. Part VI examines the choice to use cyberattacks. It demonstrates that active defenses are the most appropriate law of war response to cyberattacks, explains the technological limits to detecting, classifying and tracing cyberattacks, and explores the impact these technological limitations will have on state decision-making. Finally, Part VII, concludes the paper.

A. Cyberattacks, a Growing International Threat

The internet is essential to every modern country in the world. It is one of the cornerstones of commerce.[6] Strategic government activities are directed through it.[7] Energy production and distribution, water treatment facilities, mass transit and emergency services are controlled through it.[8] The more developed a country is, the more it depends on it.[9] Indeed, networked computers have become the nervous system of modern society.[10]

[6] *See* ANDREW COLARIK, CYBER TERRORISM, POLITICAL AND ECONOMIC IMPLICATIONS, at viii–xi (2006) (noting that trillions of dollars of electronic banking and global stock trading are conducted over it each year).

[7] *Id.* at viii–xi.

[8] *Id.* at viii–xi.

[9] *Id.* at xii.

[10] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, at vii (2003).

Global connectivity, however, is a two-edged sword. While, it provides tremendous benefits to states, it also opens the door to state and non-state actors who wish to attack and disrupt a state's critical information systems.[11] Furthermore, it is now undisputed that these attacks can have catastrophic consequences, such as bringing a state's economy to its knees, weakening its national defense posture, or causing the loss of life.[12] While these doomsday scenarios may seem farfetched, the reality is that catastrophic cyberattacks are more likely to occur as states grow more reliant on the internet,[13] as terrorists increasingly look to use cyberattacks against states,[14] and as cyberattacks become more frequent and potent.[15]

No state is safe from cyberattacks. Recent high-profile cyberattacks highlight such vulnerability. In July 2008, shortly before armed conflict broke out between Russia and Georgia, hackers barraged Georgia's internet infrastructure with coordinated cyberattacks.[16]

[11] COLARIK, *supra* note 6, at xii.

[12] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 6–7 (2003); s*ee also infra* Part II.B.

[13] *See* Richard Garnett & Paul Clarke, *Cyberterrorism: A New Challenge for International Law, in* ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 465, 487 (Andrea Bianchi ed., 2004); DANA SHEA, CONG. RESEARCH SERV. REPORT, CRITICAL INFRASTRUCTURE: CONTROL SYSTEMS AND THE TERRORIST THREAT, RL 31534, at CRS-1 to CRS-3 (2003).

[14] *See* SHEA, *supra* note 13, at CRS-6 to CRS-7; s*ee also* L. Gordon Crovitz, *Internet Attacks are a Real and Growing Problem*, WALL STREET J., Dec. 15, 2008, at 17 (describing terrorist attempts to trick military computers into mistaking the identities of friendly and unfriendly forces in Afghanistan and Iraq).

[15] *See* CLAY WILSON, CONG. RESEARCH SERV. REPORT, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS, RL 32114, at CRS-7 to CRS-8 (2007) (noting cyberattacks are growing more frequent due to the use of automated attack programs; cyberattacks now happen so often the Computer Emergency Response Team Coordination Center gave up tracking them, after tracking several hundred thousand successful attacks a year for several years); JOHN ROLLINS & CLAY WILSON, CONG. RESEARCH SERV. REPORT, TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES, RL 33123, at CRS-17 (2007) (reporting that the Department of Defense experiences more than three million scans of their computer systems each day by potential attacks, and that in according to a study by IBM in 2005, there were roughly 237 million cyberattacks conducted globally in the first half of the year); John Markoff, *Internet Attacks Grow More Potent*, N.Y. TIMES, Nov. 10, 2008, at B8 (describing the increasing capabilities of distributed-denial-of-service attacks to shut down computer systems and overcome computer defenses).

[16] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1.

The attacks overloaded and shut down many of Georgia's computer servers, and impaired Georgia's ability to disseminate information to its citizens during its armed conflict with Russia.[17] In June 2007, Chinese hackers disabled 1,500 Pentagon computers, including those of the Secretary of Defense.[18] In April 2007, cyberattacks from Russia crippled the government and commercial computer networks of Estonia.[19] These attacks lasted approximately three weeks, disrupted Estonia's ability to govern, harmed Estonia's economy, and damaged their networks so badly that Estonia had to reach out to its NATO allies to help recover from the attacks.[20] These are some of the more egregious international cyberattacks; however, there have been numerous others, often with severe consequences to the victim-states.[21] Given the potentially catastrophic consequences of cyberattacks, it is imperative for states to be able to effectively defend themselves.[22]

[17] *Id.*

[18] Mark Hosenball, *Whacking Hackers*, NEWSWEEK, Oct. 15, 2007, at 10.

[19] Mark Landler & John Markoff, *After Computer Siege on Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1; James Sterngold, *U.S. on Guard Against Computer Attacks; Estonia's Disruption Shows Need to Fortify Internet's Defenses*, SAN FRANCISCO CHRONICLE, June 24, 2007, at A4.

[20] Landler & Markoff, *supra* note 19, at A1; WILSON, *supra* note 15, at CRS-7 to CRS-8.

[21] *See, e.g.*, Christopher Rhoads, *Kyrgyzstan Knocked Offline*, WALL STREET J., Jan. 28, 2009, at 10 (discussing the January 2009 denial-of-service attacks from Russia which effectively knocked the central Asian republic of Kyrgyzstan offline); Julian Barnes, *Cyber Attack has Pentagon Worried: Russia Eyed in Hit on Defense Networks*, CHI. TRIB., Nov. 30, 2008, at C16 (discussing the November 2008 cyberattacks from Russia which disrupted U.S. Central Command's classified computer networks); Demetri Sevastopulo, *Chinese Hackers Penetrate White House Network*, FIN. TIMES ONLINE, Nov. 7, 2008, http://www.ft.com/cms/s/0/f16027f0-ac6e-11dd-bf71-000077b07658.html?nclick_check=1 (discussing the cyberattacks from China that penetrated the White House's computer network in autumn 2008, and the Obama and McCain presidential campaign networks in summer 2008); Rhys Blakely et al., *MI5 Alert on China's Cyberspace Spy Threat*, TIMES ONLINE, Dec. 1, 2007, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article2980250.ece (discussing the November 2007 cyberattacks from China against vital British commercial, governmental and military systems); Liam Tung, *China Accused of Cyberattacks on New Zealand*, CNET NEWS.COM, Sept. 13, 2007, http://news.cnet.com/China-accused-of-cyberattacks-on-New-Zealand/2100-7348_3-6207678.html (discussing the September 2007 cyberattacks from China against New Zealand's government networks); Der Spiegel Staff, *Merkel's China Visit Marred by Hacking Allegations*, DER SPIEGEL ONLINE, Aug. 27, 2007, http://www.spiegel.

B. The Legal Dilemma of State Responses to Cyberattacks

Unfortunately, state responses to cyberattacks are governed by an anachronistic legal regime, which impairs a state's ability to effectively defend itself. Right now no comprehensive treaty exists to regulate international cyberattacks or require cooperation between states.[23] Consequently, states must practice law by analogy; either equating cyberattacks to traditional armed attacks and responding to them under the law of war, or equating them to criminal activity and dealing with them as a criminal matter.[24] The prevailing view among states and legal scholars is that states must treat cross-border cyberattacks as a criminal matter because the law of war does not allow states to respond forcibly unless there is conclusive evidence that an attack was conducted by a foreign

de/international/world/0,1518,502169,00.html (discussing the August 2007 cyberattacks from China against the German chancellery, and its foreign, economy and research ministries); Roger Boyes, *China Accused of Hacking into Heart of Merkel Administration*, TIMES ONLINE, Aug. 27, 2007, http://www.timesonline.co.uk/tol/news/world/europe/article2332130.ece (discussing the August 2007 cyberattacks from China against the German chancellery, and its foreign, economy and research ministries); *see also* Richard Behar, *World Bank Under Cyber Siege in 'Unprecedented Crisis'*, FOX NEWS.COM, Oct. 10, 2008, http://www.foxnews.com/story/0%2C2933%2C435681%2C00.html (showing the vulnerability of intergovernmental organizations to cyberattacks through the Chinese cyberattacks against the World Bank).

[22] *See* Garnett & Clarke, *supra* note 13, at 488; Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection (2003).

[23] *See* AHMAD KAMAL, THE LAW OF CYBER-SPACE: AN INVITATION TO THE TABLE OF NEGOTIATIONS 170–89 (2005); Duncan Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1024–38 (2007); Jon Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations*, 9 CHI. J. INT'L L. 275, 283 (2008).

There is a Convention on Cybercrime that was adopted by the Council of Europe, which went into effect in 2004; however, it doesn't provide a comprehensive structure for dealing with cyberattacks. The United States is the only non-European nation that is a party to the convention. Notably, despite being part of the Council of Europe, Russia never entered the treaty; neither has China. *See* Council of Europe, Convention on Cybercrime, *opened for signature* Nov. 23, 2001, 41 I.L.M. 282 [hereinafter Convention on Cybercrime].

[24] *See* Hollis, *supra* note 23, at 1024–38.

government or its agents.[25] This limited view of the law of war is problematic for two reasons. First, barring forceful responses weakens state defenses to cyberattacks by prohibiting them from using active defenses.[26] Second, treating cyberattacks as a criminal matter limits state responses to passive defenses and host-state criminal laws, both of which are insufficient to protect states from cyberattacks.[27] Given these problems with the prevailing view, states will undoubtedly find themselves in a "response crisis"[28] during a cyberattack; forced to decide between effective, but arguably illegal, active defenses, and the less effective, but legal, path of passive defenses and host-state criminal laws.[29]

The current legal paradigm perpetuates the response crisis because it is virtually impossible to attribute cyberattacks at the time of attack. While states can trace cyberattacks back to computer servers inside another state, conclusively ascertaining the identity of the attacker requires intensive, time-consuming investigation, with assistance from the host-state

[25] *See* LAWRENCE GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 83–84 (1997); WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 8 n.14 (1999); Sean Condron, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 404, 414–15 (2007); Daniel Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Responding to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641, 653–54 (2002); Yoram Dinstein, *Computer Network Attacks and Self-Defense, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 111 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002).

[26] Active defenses are electronic counter-measures designed to strike the attacking system, shutting down the attacking computer system and stopping the cyberattack midstream. However, active defenses may not be used unless force is authorized under the law of war. Eric Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 230–31 (2002). Active defenses are one of the most effective defenses to cyberattacks, and can stop them in situations where passive defenses cannot. *See* Noah Shachtman, *Air Force Aims to 'Re-Write Laws of Cyberspace'*, WIRED NEWS, Nov. 3, 2008, http://blog.wired.com/defense/2008/11/air-force-aims.html; Crovitz, *supra* note 14, at 17.

[27] This shall be discussed later in this section.

[28] "Response crisis" refers to the dilemma that states face in choosing an appropriate response to a cyberattack.

[29] Adding pressure to the response crisis is that delaying the use of active defenses will increase the overall risk to a state. *See Lord: Attack Attribution, Intent are Badly Needed Cyberwar Capabilities*, 29 INSIDE THE AIR FORCE, No. 26, June 27, 2008 (quoting Major General William Lord, Commander (Prospective), Air Force Cyber Command); *see also* Condron, *supra* note 25, at 407–08 (noting that delaying the use of active defenses, so that attacks can be attributed, can result in lost lives and massive damage).

whence the cyberattack originated.[30] Given the prohibition on responding with force unless a cyberattack has been attributed to a foreign government or its agents, coupled with the fact that the vast majority of cyberattacks are conducted by non-state actors,[31] it should come as no surprise that states default to responding to cyberattacks as a criminal matter.[32] This "attribution problem"[33] locks states into the response crisis.

The link between the attribution problem and response crisis is highlighted by the same high-profile cyberattacks discussed earlier. Georgia traced the 2008 cyberattacks against it back to Russia, but couldn't pin them on its government.[34] Similarly, U.S. officials believed that China sponsored the 2007 cyberattacks against the Pentagon, but could not prove the link.[35] Following a familiar pattern, Estonia traced the 2007 attacks on it back to Russia, but could not tie them to its government.[36] Ultimately, in each of these cases states

[30] *See* Jensen, *supra* note 26, at 232–35 (discussing the difficulty of attributing cyberattacks across international borders); Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 97–99 (2001) (noting that attributing cyberattackers cannot be done without extensive investigation, in which access to the originating servers is granted by the host-state's government).

[31] Jensen, *supra* note 26, at 232.

[32] *See* Condron, *supra* note 25, at 407 (noting the United States treats international cyberattacks as a criminal matter); Hollis, *supra* note 23, at 1050 (noting that Estonia responded to the 2007 cyberattacks from Russia through diplomatic channels, despite their belief that Russia sponsored the attacks, because of the legal requirement to attribute cyberattacks before treating them as violations of the law of war).

[33] "Attribution problem" refers to the difficulty of ascertaining the identity of cyberattackers.

[34] Markoff, *supra* note 16, at A1. Evidence obtained much later suggests that a criminal gang, known as the Russian Business Network, was behind the cyberattacks, possibly with the support of the Russian government; however, Moscow has denied any involvement. *Id.* *See generally* Eneken Tikk et al., *Cyber Attacks against Georgia: Legal Lessons Identified*, NATO COOPERATIVE CYBER DEFENSE CENTER OF EXCELLENCE (2008) (providing more detailed information on the cyberattacks).

[35] Demetri Sevastopulo, *Chinese Hacked into Pentagon*, FIN. TIMES ONLINE, Sept. 3, 2007, http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html; Demetri Sevastopulo, *Beware: Enemy Attacks in Cyberspace*, FIN. TIMES ONLINE, Sept. 3, 2007, http://www.ft.com/cms/s/0/a89c1c88-5a38-11dc-9bcd-0000779fd2ac.html.

[36] Landler & Markoff, *supra* note 19, at A1.

were unable to solve the attribution problem; legally limiting them from using active defenses, and forcing them to rely on passive defenses and host-state criminal laws.

The requirement to treat cyberattacks as criminal matters wouldn't be problematic if passive defenses and host-state criminal laws provided sufficient protection to cyberattacks. Unfortunately, neither is adequate. Passive defenses, also known as computer security, are always the first line of defense against cyberattacks.[37] However, while passive defenses reduce the chance of a successful cyberattack, as the attacks discussed so far show, and as security experts will tell you, even with good computer security, it is difficult to completely secure a state's critical information systems.[38] Furthermore, passive defenses do little to dissuade attackers[39] from attempting their attacks in the first place.[40] Deterrence comes from criminal laws and the penalties associated with them.[41] However, when host-states fail to pass stringent criminal laws or look the other way when cyberattacks are conducted against

[37] *See* LEHTINEN ET AL., COMPUTER SECURITY BASICS 3–21 (2d ed. 2006); COLARIK, *supra* note 6, at 10.

[38] *See* COLARIK, *supra* note 6, at 163.

[39] Up to this point, the term hacker has been used to generically refer to anyone conducting a cyberattack. However, from here on, this paper will either use the more appropriate term "attacker" to generally refer to individuals who conduct cyberattacks, or one of the more specific terms: "hacker," "cracker," "cybercriminal" and "cyberterrorist." Hackers are anyone with an eagerness to experiment with computers and test their limits. Crackers are hackers who unlawfully break into systems; usually for the thrill of it, but also to peek at interesting data contained in the systems targeted. Cybercriminals are crackers who go one step further and use their cyberattacks to steal and sell data, embezzle money, or engage in extortion. Cyberterrorists employ cyberattacks to create fear or violence through the destruction or disruption of computer systems, as a means of influencing a government or population to conform to a particular political or ideological agenda. *See* LEHTINEN ET AL., *supra* note 37, at 16–17; COLARIK, *supra* note 6, at 37–48.

[40] In the case of hackers and crackers, beating security measures is often seen as a fun challenge. *See* LEHTINEN ET AL., *supra* note 37, at 16–17; Frontline: Hacker Interviews, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/ (last visited Mar. 22, 2009). Furthermore, the more secure a system is, the more difficult it is for an attacker to penetrate the system's defenses; however, defensive measures alone pose little risk to the attacker. While defensive measures can trace attacks back to their source, absent stringent criminal laws and vigorous law enforcement, defensive measures cannot harm an attacker. *See* COLARIK, *supra* note 6, at 40–45.

[41] *See* COLARIK, *supra* note 6, at 39 (explaining the importance of criminal laws with clear penalties to deter hackers from breaking into computer systems).

rival states, host-state criminal laws are rendered impotent.[42] Unfortunately, several major states refuse to take part in international efforts to prosecute cyberattacks and seem unlikely to start doing so in the near future.[43] For instance, despite Chinese and Russian pledges to crackdown on their attackers,[44] no one has ever been brought to justice for any of the attacks discussed. This suggests that China and Russia are intentionally avoiding bringing their hackers to justice. For example, instead of working to deter international cyberattacks, China is, in fact, training its hackers to bypass computer defenses at Chinese military academies.[45] Furthermore, security experts believe that China is intentionally ignoring the criminal acts of its hackers, buying stolen information from them, and using them to spy on other states.[46] Meanwhile, Russia has rejected numerous Estonian requests to help track down the attackers

[42] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 8 (2003). State cooperation is essential to the criminal prosecution of international attackers. *Id.* However, state cooperation relies on the goodwill of nations. For instance, even when an attacker has been identified, the host-state may refuse to prosecute or extradite them back to the victim-state. Such obligations only arise from international treaties that set forth state responsibilities. *See* Factor v. Laubenheimer, 290 U.S. 276, 287 (1933); GREENBERG ET AL., *supra* note 25, at 69–72; KAMAL, *supra* note 23, at 215–22.

Obtaining state cooperation often requires intense diplomatic activity, which presents its own challenges to relying on host-state criminal laws. For instance, diplomatic activity is usually required to get a host-state to prosecute an attacker under their criminal laws, or to get a host-state to turn over an attacker so that he can be prosecuted under victim-state's criminal laws; neither of which can be required absent a treaty requiring such action. It is worth noting that the United States does not have extradition treaties with China or Russia, and thus no legal right exists to demand the extradition from those states. *See* Creekman, *supra* note 25, at 658.

[43] *See* Condron, *supra* note 25, at 414.

[44] *See* Richard McGregor & Hugh Williamson, *Beijing Pledges Crackdown on International Hackers*, FIN. TIMES ONLINE, Aug. 28, 2007, http://www.ft.com/cms/s/0/9b4cfc4e-54fe-11dc-890c-0000779fd2ac.html; Iain Thomson, *Russia Promises Piracy Crackdown*, VNUNET.COM, Mar. 19, 2007, http://www.vnunet.com/vnunet/news/2185839/russia-promises-piracy (reporting Russia's pledge to crackdown on online criminal activity).

[45] *See generally* U.S. - CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2008 REPORT TO CONGRESS (2008), *available at* http://www.uscc.gov (describing China's initiatives to augment its cyberwarfare capabilities to gain an advantage over the United States in any future conflict, amid other economic and security concerns).

[46] *See* Bruce Schneier, *Chinese Cyber Attacks*, July 14, 2008, http://www.schneier.com/blog/archives/2008/07/chinese_cyber_a.html (speculating that China knows its leading hackers, intentionally ignores their international crimes, and even buy stolen intelligence from them).

responsible for the 2007 cyberattacks against it.[47] As may be expected, China and Russia reject these accusations.[48] Still, the failure of China and Russia to produce any results from their "crackdowns" suggests that state cooperation is offered in name only, raises the specter of state sponsorship of the attacks, and suggests that host-state criminal laws are inadequate to answer the growing cyberthreat. Furthermore, even stringent criminal laws and vigorous law enforcement are unlikely to completely deter terrorists from committing cyberattacks due to the extreme ideologies that drive them. The foregoing discussion illustrates the need to ascertain what states may legally do to defend themselves against cyberattacks.

C. Solving the Legal Crisis

The obvious way to escape this dilemma is for states to use active defenses. Not only can active defenses hinder an ongoing attack, but it logically follows that attackers will hesitate to attack a state when they know their attacks will be met with a forceful response. After all, it is generally recognized that "[m]aintaining a credible ability to use force, in cyberspace and elsewhere, is . . . a fundamentally important aspect of deterrence."[49] But can states legally act in this manner? And if so, is this the best way to address the cyberthreat?

[47] *See* Hollis, *supra* note 23, at 1026. Lending credence to Estonian assertions that Russia is intentionally obstructing the criminal investigation into the cyberattacks is the fact that the Russian public has hailed the hackers responsible for the cyberattacks against Estonia as national heroes. *See* Clifford Levy, *What's Russian for 'Hacker'?*, N.Y. TIMES, Oct. 21, 2007, at Week In Review, p. 1.

[48] Associated Press, *China Dismisses U.S. Espionage Report as Misleading*, Nov. 22, 2008, *available at* http://www.google.com/hostednews/ap/article/ALeqM5jzzULJt2ZiW2IZR3KKuViEpbOAlQD94JTGS80; Richard McGregor & Demetri Sevastopulo, *China Denies Hacking into Pentagon*, FIN. TIMES ONLINE, Sept. 4, 2007, http://www.ft.com/cms/s/0/a625db16-54c4-11dc-890c-0000779fd2ac.html; Hollis, *supra* note 23, at 1026.

[49] SHARP, SR., *supra* note 25, at 135; THOMAS WINGFIELD, THE LAW OF INFORMATION CONFLICT, NATIONAL SECURITY LAW IN CYBERSPACE 361 (2000).

History has shown us that states will take matters into their own hands when legal means seem inadequate to protect themselves and their citizens.[50] While no cyberattack has yet risen to a level where a state felt it must resort to force to defend itself, it is not hard to imagine a scenario where a state was subject to a cyberattack so severe that it felt an armed response was required. Given the ease with which a non-state actor could trigger such a scenario, it is imperative for international law to provide states acceptable legal means to defend themselves. When international law provides states acceptable legal means to resolve their disputes, states are more likely to behave in predictable ways that are accepted by the international community.[51] Thus, unless the international community wants to risk states responding to cyberattacks in unpredictable and potentially unacceptable ways, international law must adapt to provide states with legal means to effectively defend themselves.

This is not a new thought. There is a growing recognition among legal scholars that the current legal regime leaves states vulnerable to cyberattacks and needs to change.[52]

[50] This happened as recently as 2008, when the United States authorized its military to carry out air and ground assaults against Al Qaeda inside other states without the approval of their governments. Since then, the United States has conducted raids inside Pakistan and Syria against their wishes. The United States has justified its actions as self-defense due to those states' inability or unwillingness to handle the terrorists, despite evidence suggesting that Pakistan and Syria are cooperating and having some success with their counter-terrorism efforts. *See* Eric Schmitt & Mark Mazzetti, *Bush Said to Give Orders Allowing Raids in Pakistan*, N.Y. TIMES, Sept. 11, 2008, at A1; Jane Perlez, *Pakistan's Military Chief Criticizes U.S. Over a Raid*, N.Y. TIMES, Sept. 11, 2008, at A8; Eric Schmitt & Thom Shanker, *Officials Say U.S. Killed an Iraqi in Raid in Syria*, N.Y. TIMES, Oct. 28, 2008, at A1; Eric Schmitt & Mark Mazzetti, *Secret Order Lets U.S. Raid Al Qaeda*, N.Y. TIMES, Nov. 10, 2008, at A1; Ismail Khan & Jane Perlez, *Airstrike Kills Militant Tied to Al Qaeda in Pakistan*, N.Y. TIMES, Nov. 23, 2008, at A10.

When states take matters into their own hands, they tend to justify their actions under the mantle of law, even when they fail to meet the accepted legal threshold. This is done as a tactical measure to secure the broadest possible support for their actions. Though at times, the states actually believe their actions are legal. Sean Murphy, *The Doctrine of Preemptive Self-Defense*, 50 VILL. L. REV. 699, 727–31 (2005).

[51] *See* Murphy, *supra* note 50, at 704–05.

[52] Garnett & Clarke, *supra* note 13, at 488; GREENBERG ET AL., *supra* note 25, at 99–100; KAMAL, *supra* note 23, at 83–84; Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information*

However, despite their recognition of the problem, no consensus has emerged on the best way to solve it. Some scholars advocate new treaties to get past this legal shortcoming. For example, one proposal calls for a treaty requiring states to rebuild the internet's architecture in a more secure manner, so that law enforcement can easily track attackers.[53] Another proposal calls for a comprehensive international treaty to regulate cyberattacks.[54] Other scholars advocate changing the law of war to allow states to respond to cyberattacks with active defenses without having to attribute cyberattacks to a state. Thus, one scholar proposed exempting states from having to attribute attacks against their critical infrastructure.[55] Another proposed that attributing attacks is unnecessary because states can legally respond to attacks by non-state actors with force under customary international law (CIL).[56] While these approaches are all preferable to the current legal paradigm, there are shortcomings with each of them, which this paper will address.[57]

The legal key to authorizing active defenses is a state's duty to prevent non-state actors within their borders from committing cross-border cyberattacks. "It is a long established principle of international law that 'a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another state or its

Systems in Armed Conflict, 47 HARV. INT'L L.J. 179, 181–83 (2006); Condron, *supra* note 25, at 415–16; Hollis, *supra* note 23, at 1023.

[53] *See generally* LAWRENCE LESSIG, CODE: VERSION 2.0 (2006).

[54] *See generally* Brown, *supra* note 52, at 179.

[55] *See* Jensen, *supra* note 26, at 236–37; Condron, *supra* note 25, at 415–22.

[56] *See* Barkham, *supra* note 30, at 104; Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 933–34 (1999). This proposal would allow states to use active defenses regardless of who is conducting the cyberattack.

[57] *See infra* note 172 and accompanying text (discussing the shortcomings of treaty based solutions); *infra* note 386 and accompanying text (discussing the shortcomings of the current proposals to change the law of war).

people.'"[58] Traditionally, this duty only required states to prevent illegal acts that the state knew about beforehand; however, this duty has evolved in response to international terrorism to require states to act against groups generally known to carry out illegal acts.[59] In the realm of cyberwarfare, states must take this duty one step further and interpret it to require them to take affirmative steps to protect each other from and hold their citizenry liable for international cyberattacks. Otherwise, the current situation that states face with China and Russia will continue to exist. While no international treaty affirmatively obligates a state to hunt down attackers within their borders, such as with piracy,[60] re-structuring the duty of prevention to require states to hunt down attackers will solve the attribution problem and response crisis. Once this duty is restructured, international law allows victim-states to impute state responsibility to host-states that neglected this duty, and respond in self-defense.[61] In effect, repeated failure by a state to enforce its criminal laws will result in that state being declared a sanctuary state, allowing victim-states to use active defenses against any cyberattack originating from within the host-state's borders.

Selectively targeting sanctuary states with active defenses should also provide the added benefit of getting sanctuary states to start taking cyberattacks seriously as a criminal matter. Since no state wants another state acting within its borders, even electronically, this

[58] Michael Schmitt, *Preemptive Strategies in International Law*, 24 MICH. J. INT'L L. 513, 540–41 (2003) (quoting S.S. Lotus (Fr. V. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7, 1927) (Moore, J., dissenting), and referring to numerous state pronouncements to that effect with regard to international terrorism).

[59] *See infra* Part IV.B (discussing the traditional and contemporary views of a state's duty to prevent non-state actors within their borders from committing cross-border criminal acts).

[60] *See* U.S. DEP'T OF THE NAVY, NWP 1-14M, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS § 3.5 (2007) [hereinafter COMMANDER'S HANDBOOK] (referencing international law's longstanding obligation for states to repress piracy; and quoting the 1958 Geneva Convention on the High Seas and the 1982 Law of the Sea Convention).

[61] *See infra* Part IV–V.

restructured duty should motivate states to hunt down attackers within their borders and work with victim-states to bring them to justice. States who wished to avoid being the targets of active defenses could easily do so; all they would have to do is pass stringent criminal laws, conduct vigorous and transparent criminal investigations, and prosecute attackers.[62]

II. Examining Cyberattacks

Before fully exploring the legal regime governing cyberattacks, one must first understand this unique form of modern warfare. Effective regulation requires an understanding of the conduct it seeks to regulate. Attempting to regulate a subject without understanding it can easily lead to ineffective regulations that fail to accomplish their intended purpose. This paper shall, therefore, examine cyberattacks, their potential impact, and the defenses against them, as a precursor to exploring the legal regime governing them.

A. Types of Cyberattacks

Cyberattacks come in many different forms. To generalize, there are three main categories of cyberattacks.[63] The first category is automated malicious software delivered

[62] *See infra* Part V.B–C.

[63] Cyberattacks can be categorized in different ways. It is this author's opinion that there are three main categories of cyberattacks. However, other authors categorize cyberattacks into as little as two or as many as four main categories. *See* LEHTINEN ET AL., *supra* note 37, at 79–95, 112–133 (categorizing cyberattacks into viruses and internet vulnerabilities); COLARIK, *supra* note 6, at 84 (categorizing cyberattacks into viruses, denial-of-service attacks, web defacements and unauthorized penetration).

over the internet.[64] The second category is denial-of-service (DOS) attacks.[65] The third category is unauthorized remote intrusions into computer systems by individuals.[66]

It is worth noting cyberattacks can originate locally rather than remotely over the internet. For instance, malicious software may be locally loaded onto a system via a storage device, such as a thumb drive or computer disc, and unauthorized intrusions may originate at a physical terminal connected to a computer network. However, while computer systems are more vulnerable to internal penetration at their physical location, this paper is focused on external cyberattacks conducted via the internet across international borders.[67]

Malicious code or malware, as it's known inside computer circles, usually infects computer systems through infected emails, vulnerability exploit engines or visits to infected websites.[68] Early malware fell into two main classifications, viruses and worms.[69] Viruses

[64] *See* COLARIK, *supra* note 6, at 84.

[65] *See id.*

[66] *See id.*

[67] Internal penetrations are a serious issue despite not being the focus of this paper. Authorized users, also known as insiders, have greater access to computer systems than unauthorized users. This access makes it easy for them to load malicious code onto a system, or to do something beyond their authorization. *See* COLARIK, *supra* note 6, at 85–86. Internal penetrations can be inadvertent or intentional. In the case of an inadvertent penetration, a user might connect an infected storage device to a computer network, which then executes its code to the detriment of the system. In the case of an intentional penetration, a user could simply use their access to conduct harmful acts within their access rights, or attempt to use their limited access to try to gain greater access to the system and then conduct harmful acts. *See* LEHTINEN ET AL., *supra* note 37, at 96–111.

However despite being a cyberattack of sorts, internal penetrations should fall under domestic law, as the cyberattack occurs as a result of a physical act at the location of the computer networks. This puts internal penetrations squarely in the domestic jurisdiction of the state in question. Absent an intentional act by a member of a transnational terrorist organization, who happens to have gained local access to a computer system, there is no international character to the penetration. In the case that such an act is committed by a transnational terrorist, some of the concepts discussed in this paper may be appropriate for analogy.

[68] LEHTINEN ET AL., *supra* note 37, at 79; COLARIK, *supra* note 6, at 84.

[69] LEHTINEN ET AL., *supra* note 37, at 80. These definitions were derived from the methods the programs used to carry out an attack. *Id.*

are code fragments that copy themselves into larger programs, modifying those programs to carry out functions than those originally intended.[70] The virus is dependent on the main program, and cannot execute until the main program is run.[71] Once the main program is run, viruses load themselves into the memory of the computer system once and execute their code.[72] A virus then replicates itself, infecting other programs and files.[73] After it finishes reproducing, it carries out whatever dirty work is in its programming, called delivering a payload.[74] Worms are self-sustaining independent programs that reproduce themselves by copying themselves in full-blown fashion from one computer to another via a network or the internet.[75] Worms can spread rapidly from system to system, copying themselves to any computer systems connected to the infected computer and if programmed to do so, delivering their payload on the new system after replicating themselves.[76]

As computer programs became more sophisticated, classifying malware by their attack method failed to adequately describe the diverse nature of viruses and worms.[77] As a result, these categories were further defined by their function.[78] The most common subdivisions of viruses and worms are Trojan horses, rootkits, sniffers, exploits, bombs and

[70] *Id.* at 81–82.

[71] *Id.*

[72] LEHTINEN ET AL., *supra* note 37, at 82; COLARIK, *supra* note 6, at 91.

[73] LEHTINEN ET AL., *supra* note 37, at 82; COLARIK, *supra* note 6, at 91–92.

[74] LEHTINEN ET AL., *supra* note 37, at 82.

[75] *Id.* at 85.

[76] LEHTINEN ET AL., *supra* note 37, at 85; COLARIK, *supra* note 6, at 92.

[77] LEHTINEN ET AL., *supra* note 37, at 80.

[78] *Id.*

zombies.[79] Attackers may choose a single one of these programs or use them in conjunction with each other.[80] The only limit to the complexity of an attack is the imagination of the attacker. Additionally, attackers may also use malware in conjunction with DOS attacks and unauthorized remote intrusions.[81]

Denial-of-service (DOS) attacks use the communication protocols that allow computers to communicate with one another against them, overwhelming the targeted computer system with information until it seizes up and ceases to function.[82] This effectively denies the availability of the targeted system to legitimate users.[83] DOS attacks can use malformed packets to overwhelm a system's processors, or flood the processor with so many data requests that it overwhelms the system itself or its supporting network bandwidth.[84] The

[79] LEHTINEN ET AL., *supra* note 37, at 80–81. Trojan horses trick a user into running a program that appears to be beneficial, but actually has a code fragment hidden inside the program, which performs a disguised function. *Id.* at 87. Rootkits install new accounts on a computer system or steal existing account information, and then elevate the security level of those accounts to the highest degree so that the attacker can later enter at will without obstruction. *Id.* at 81, 87. Sniffers monitor the keystrokes of authorized users and send the stolen information back to a storage facility for later access by the program designer. *Id.* at 81, 88. Exploits are programs that capitalize on known or undiscovered system vulnerabilities, such as weaknesses in a piece of software or the operating system, to gain access to the system and execute their program. *Id.* at 81, 87. Exploits may also capitalize on system vulnerabilities created through poor security practices and procedures, in addition to those created by technical errors. *See* WILSON, *supra* note 15, at CRS-25. Bombs are programs that destroy data by reformatting the hard disc or inserting corrupted files by inserting random data into them. U.S. ARMY TRAINING AND DOCTRINE COMMAND, DCSINT HANDBOOK NO. 1-02, CRITICAL INFRASTRUCTURE THREATS AND TERRORISM VII-7 (2006) [hereinafter CRITICAL INFRASTRUCTURE THREATS]. Bombs can execute immediately after being loaded onto a system or be delayed to go off at a later date. LEHTINEN ET AL., *supra* note 37, at 88. Time bombs can be set to go off at a specific time; logic bombs can be set to go off after a particular event occurs. *Id.* at 88. Zombies are malware that entrenches itself inside a computer system and then lays low until its master triggers it into action. *Id.* at 81, 83.

[80] *See* LEHTINEN ET AL., *supra* note 37, at 79–95. For example, an attacker may use a Trojan horse to deliver a rootkit or sniffer, or may use an exploit to implant a zombie.

[81] *Id.*

[82] *See* LEHTINEN ET AL., *supra* note 37, at 81; COLARIK, *supra* note 6, at 84, 103.

[83] LEHTINEN ET AL., *supra* note 37, at 12.

[84] *See* COLARIK, *supra* note 6, at 103.

most severe form of DOS attack is a distributed denial-of-service (DDOS) attack.[85] DDOS attacks are DOS attacks launched simultaneously from numerous computers.[86] The sheer volume of a DDOS attack makes it extremely difficult to defend against.[87] In addition to being able to cripple computer systems attached to the internet, DOS attacks can overwhelm system defenses, such as knocking down a firewall, so that the system becomes vulnerable to other forms of attack.[88]

Unauthorized remote intrusions are external penetrations of a computer system by an individual.[89] The key point here is that this category of cyberattack has an intelligent being on the other end of the connection directing the cyberattack. The attack process for these "cyberattacks [is] not unlike other attack methodologies."[90]

[85] *See id.*

[86] LEHTINEN ET AL., *supra* note 37, at 81. DDOS attacks are usually launched from zombies, which attackers hijack ahead of time. These virtual networks of zombies all being directed at once for a single nefarious purpose are known as Botnets. It is not unheard of to have several hundred thousand zombies, or Bots, harnessed at once to unleash one coordinated massive attack. Botnets can be used to deliver malicious code, gather information or conduct DDOS attacks. *See* WILSON, *supra* note 15, at CRS-5 to CRS-7.

An interesting evolution of DDOS attacks occurred in 2007 with the "e-Jihad" computer program. e-Jihad let computer owners freely give control of their system to the creators of e-Jihad, who agreed to use their computers to attack anti-Islamic entities. e-Jihad would coordinate the attacks of the freely lent computers, effectively turning them into a network of zombies, and report back to the owners on the success rates of the attacks. e-Jihad has since been shut down, but there will inevitably be similar programs in the future. *See* Larry Greenemeier, *'Electronic Jihad' App Offers Cyberterrorism for the Masses*, INFORMATIONWEEK.COM, July 2, 2007, http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=200001943.

[87] *See* COLARIK, *supra* note 6, at 103.

[88] COLARIK, *supra* note 6, at 103. Web-based attacks, such as a DOS attack, can be used to cause a buffer overflow in the memory of the targeted computer. Buffer overflows of the computer's stack, the part of memory used for temporary variable storage, can cause the computer to write the overflow of data to the computer's heap, the segment of memory that stores code waiting for execution. This is called "smashing the stack." Smashing the stack allows attackers to implant executable programs into the targeted computer to gain further access. Imagine a rootkit being implanted this way. *See* LEHTINEN ET AL., *supra* note 37, at 131–32.

[89] *See* COLARIK, *supra* note 6, at 94.

[90] *Id.* at 83.

> The first phase of an attack is reconnaissance of the intended victim. By observing the normal operations of a target, useful information can be ascertained and accumulated such as hardware and software used, regular and periodic communications, and the formatting of said correspondences. The second phase of an attack is penetration. Until an attacker is inside a system, there is little that can be done to the target except disrupt the availability or access to a given service provided by the target. . . . The third phase is identifying and expanding their internal capabilities by viewing resources, and increasing access rights to more restricted, higher-value areas of a given system. The fourth stage is where the intruder does the damage to the system, or confiscates selected data and/or information. The last phase can include the removal of any evidence of a penetration, theft, and so forth by covering the electronic trail by editing or deleting log files. Ultimately, the intruder wants to complete all five stages successfully.[91]

Initial system penetration frequently occurs before an attacker ever personally accesses a system. This is typically achieved through malware, which increases an attacker's access rights. However, when penetration has yet to occur, attackers may attempt to access a system by pretending to be an authorized user logging on remotely. Remote logins occur at user access points and require user account names and passwords.[92] Attackers use social engineering, packet sniffers and password cracking to acquire such information.[93] Once an attacker accesses a system, the attacker can do a variety of harmful things with or to the

[91] *Id.*

[92] *See id.* at 97.

[93] *See* COLARIK, *supra* note 6, at 97–98. Social engineering tricks users into giving away their account information. This often happens when attackers impersonate company employees or system administrators over the phone. *Id.* at 94. Packet sniffers capture user data being transmitted to/from a system. *Id.* at 97–98. Password cracking comes in two forms, brute force and dictionary attacks. Brute force attacks guess passwords "by trying every possible combination of characters, one attempt at a time." Dictionary attacks guess passwords by using commonly used words or variations thereof. Dictionary attacks are often aided by advance reconnaissance, as many people pick easy passwords, such as their initials or children's names. LEHTINEN ET AL., *supra* note 37, at 61.

system, including “caus[ing] people or processes to act on the changed data in a way that causes a cascading series of damages in the physical and electronic world.”[94]

B. Potential Impact of Cyberattacks

The internet’s open architecture makes it “ideally suited for asymmetrical warfare.”[95] Cyberattacks “can be used by both states and non-state actors to anonymously pry into a state’s public, sensitive and classified computers . . . to manipulate data; to deceive decision makers; to influence public opinion; and even to cause physical destruction from remote locations abroad.”[96] Cyberattacks overcome the requirement for conventional military forces, allowing attackers who understand computer systems to inflict damage on another state, anonymously and for minimal cost, from the other side of the globe.[97]

Attackers can direct cyberattacks at any computer system connected to the internet; however, the most dangerous attacks are those against critical national infrastructure (CNI).[98] CNI systems are so essential to a state’s well being that states have sworn to protect them

[94] COLARIK, *supra* note 6, at 84.

[95] WINGFIELD, *supra* note 49, at 21.

[96] *Id.* at 21–22.

[97] *See id.* at 22.

[98] *See* Timothy Shimeall et al., *Countering Cyber War*, 49 NATO REV. 16, 17–18 (Winter 2001/2002), *available at* http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf (noting cyberattacks on CNI would likely result in significant loss of life, and economic and social degradation). While cyberattacks against CNI are the most dangerous form of cyberattack, lesser attacks are still destructive. For instance, the FBI recently estimated that cybercrime, a subset of cyberattacks, causes an average financial loss of $167,713 per attack, and as a whole have caused over $400 billion in damages in the United States. WILSON, *supra* note 15, at CRS-27 to CRS-29.

regardless of whether the systems are civilian or governmental.[99] While there is no inclusive list of CNI, a functional analysis of the role that computers play in key resource sectors shows that computer systems form the backbone of almost every nationally significant sector, including: banking and finance, communications, energy, emergency services, government, transportation, and water supply systems.[100] Cyberattacks against these sectors can intimidate populations, damage the economy, and even injure or kill.[101] Furthermore, cyberattacks provide terrorists a way to increase the destructive impact of physical attacks.[102] In essence, cyberattacks are just another tool for a state's enemies to use against it.

Cyberattacks can terrorize a population, just like normal terrorist attacks. The National Security Agency has demonstrated that cyberattacks can disrupt operations at major military commands, cause large-scale blackouts, and interrupt phone service across the United States.[103] Furthermore, much of the United States' CNI is controlled by Supervisory Control and Data Acquisition (SCADA) systems, which are particularly vulnerable to cyberattacks.[104] When cyberattacks shut down these systems, people, businesses and

[99] *See* Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection (2003); Condron, *supra* note 25, at 404–07; Jensen, *supra* note 26, at 226–28; JOHN MOTEFF, CONG. RESEARCH SERV. REPORT, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION, RL 30153, at CRS-3 to CRS-13 (2008).

[100] *See generally* Department of Homeland Security, Critical Infrastructure and Key Resources, http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm (last visited Mar. 22, 2009) (detailing the different sectors of critical national infrastructure and explaining their interrelations).

[101] *See* COLARIK, *supra* note 6, at 15–28 (2006).

[102] *See* COLARIK, *supra* note 6, at 51–52; WILSON, *supra* note 15, at CRS-21.

[103] *See* WINGFIELD, *supra* note 49, at 24–25 (discussing the 1997 *Eligible Receiver* military exercise).

[104] WILSON, *supra* note 15, at CRS-21 to CRS-23. SCADA systems are often remotely located and unmanned, but still connected to the internet to perform their command and control functions. *Id.* They are used to manage public and private utilities, and much of the communications infrastructure. COLARIK, *supra* note 6, at 122.

government can be deprived of basic services, which can cause panic in a populace, effectively turning these cyberattacks into a means of scaring a population, potentially for political ends.[105] Another vulnerability of corporate, government, and military critical systems is their frequent reliance on Commercial-Off-The-Shelf (COTS) hardware and software.[106] COTS systems are more vulnerable to penetration than specially designed systems, making them easier to exploit, more susceptible to damage, and likely to lead to harm to a state and its citizens.[107] Intimidating populations via cyberattacks is just another way for terrorists to sow terror.

The potential economic consequences of cyberattacks are just as profound. Cyberattacks have the potential to cripple a state's commercial infrastructure, such as a stock exchange, and bring the state's economy to its knees.[108] Cyberattacks on the underlying economic infrastructure of a state are an attractive method of warfare for terrorists because so much of a state's economy is facilitated by telecommunications and computer systems.[109] Successful terrorist attacks on banking and finance CNI have the potential to undermine

[105] *See* COLARIK, *supra* note 6, at 19–20, 118–24 (2006). The vulnerability of SCADA systems has been demonstrated many times. In 2003, the "Slammer" worm shut down the control systems of an Ohio nuclear power plant. WILSON, *supra* note 15, at CRS-22. Also in 2003, the "Blaster" worm interrupted the warning systems of the northeastern power grid and contributed to the 2003 blackout across the eastern United States. *Id.* at CRS-23. In 2007, the Aurora Generator Test conducted by Idaho National Laboratories demonstrated that coordinated cyberattacks can overheat and shut down power turbine generators. *Id.* at CRS-19 to CRS-20. Furthermore, security experts believe that Chinese cyberattacks contributed to two blackouts in the United States. The first was the northeastern blackout in 2003; the second was the Daytona Beach and Monroe County, Florida blackout in February 2008. Shane Harris, *China's Cyber-Militia*, NAT'L J., May 31, 2008, cover story.

[106] WILSON, *supra* note 15, at CRS-23 to CRS-24; COLARIK, *supra* note 6, at 130.

[107] WILSON, *supra* note 15, at CRS-24. Government use of COTS systems have already resulted in the infiltration of top-secret computer systems on more than one occasion. *Id.*

[108] WINGFIELD, *supra* note 49, at 24–25; COLARIK, *supra* note 6, at 139.

[109] *See* COLARIK, *supra* note 6, at 124–28.

confidence in a state's economic infrastructure, and increase the costs of doing business to the point that doing such business becomes commercially infeasible.[110] At a time when tens of trillions of dollars are held by international banks, worldwide annual credit card purchases nearly reach $2 trillion, U.S. finance and insurance companies comprise $905 billion of the gross domestic product, and online sales in the United States already amount to hundreds of billions per annum, all of which are dependent on cyberspace, cyberattacks provide an extremely attractive method of attack for a states' enemies.[111]

Cyberattacks also have the potential to injure or kill, directly or indirectly, when used as a force multiplier in conjunction with physical attacks.[112] Cyberattacks directed against the transportation sector, for example, could crash airplanes,[113] or cause trains to collide.[114] The transportation sector relies heavily on SCADA and COTS systems, and has already proven vulnerable to cyberattacks.[115] Cyberattacks could also be directed against dams, causing floodgates to open,[116] or chemical and liquid natural gas plant control systems,

[110] *See id.* at 22.

[111] *See* COLARIK, *supra* note 6, at 124–28 (reviewing commerce over the internet); WILSON, *supra* note 15, at CRS-21 (referencing Chinese military journals, which claim the ability to bring down U.S. financial markets with cyberattacks); U.S. Census Bureau, The 2009 Statistical Abstract: Online Retail Sales, http://www.census.gov/compendia/statab/cats/ wholesale_retail_trade/online_retail_sales.html (recording $128.1 billion in online sales in 2007 and projecting online sales to rise to $147.6 billion in 2008, in the Online Retail Spending report).

[112] *See* CRITICAL INFRASTRUCTURE THREATS, *supra* note 79, at VII-7.

[113] *See* COLARIK, *supra* note 6, at 128–30.

[114] *See* CRITICAL INFRASTRUCTURE THREATS, *supra* note 79, at VII-1 (noting the railroad signal and switching system could be manipulated to cause trains to crash into each other).

[115] While no one was hurt when it happened, hackers have previously taken over and shut off a regional airport's control tower and runway lights. COLARIK, *supra* note 6, at 130.

[116] *See* WILSON, *supra* note 15, at CRS-21.

which could easily lead to widespread physical damage or death.[117] To illustrate these points, in 2000 a cyberattack took control of a sewage plant in Maroochy Shire, Australia, and dumped 264,000 gallons of untreated sewage into the local environment.[118] Cyberattacks could also directly target medical systems, altering critical medical information, such as blood types, immunization histories, allergies, or other critical data.[119] "The modification of such details could cause the medical practitioners to diagnose a course of treatment that could be fatal to the patient."[120] However, the scenario that concerns experts the most is the use of cyberattacks against electronic emergency warning and response systems in conjunction with physical attacks.[121] When attackers use cyberattacks to degrade state defenses to physical attacks in this manner, they exponentially amplify the likely total damage from a physical attack.[122] Given the devastating impact that cyberattacks can have on a population's sense of security, economic well-being and safety, it is imperative for states to defend themselves with the best computer defenses allowed under the law.

C. Defenses against Cyberattacks

[117] SHEA, *supra* note 13, at CRS-8.

[118] *Id.* at CRS-7.

[119] COLARIK, *supra* note 6, at 131.

[120] *Id.*

[121] SHEA, *supra* note 13, at CRS-9.

[122] COLARIK, *supra* note 6, at 138–40; CRITICAL INFRASTRUCTURE THREATS, *supra* note 79, at VII-7; SHEA, *supra* note 13, at CRS-9. Furthermore, evidence indicates that terrorists are conducting cybersurveillance on U.S. critical infrastructure for this purpose. SHEA, *supra* note 13, at CRS-6 to CRS-7.

Today, computer security comes in four general categories: system access controls, data access controls, security administration, and secure system design,[123] which are also known as passive defenses.[124] These defenses function on the general axiom of computer security that states can limit the damage from cyberattacks by reducing an attacker's ability to gain unauthorized access to a computer system.[125] The more secure a system is designed, the more difficult it is for attackers to penetrate the system and cause harm.[126] However, computer security has a potential fifth category: active defenses.[127] The difference between passive defenses and active defenses is that passive defenses do not use force, and as a result, are considered lawful under international law.[128] Active defenses, on the other hand, employ electronic force, and may only be used when force is authorized under the law of war.[129] So far, states have confined their computer security to passive defenses, as active defenses are forbidden under the prevailing view of the law of war.[130] However, all five categories of computer security provide states with essential tools to protect themselves from cyberattacks.

[123] LEHTINEN ET AL., *supra* note 37, at 49–50.

[124] *See* Jensen, *supra* note 26, at 230.

[125] *See* COLARIK, *supra* note 6, at 83 (noting that without access, all an attacker can do is shut down a system or prevent access to it).

[126] *See* LEHTINEN ET AL., *supra* note 37, at 49 (noting that computer security makes sure computers do what they're supposed to do by protecting the data stored in a computer from being read, destroyed or modified by those without authorized access).

[127] *See* Jensen, *supra* note 26, at 230.

[128] *Id.*

[129] *Id.* at 231.

[130] *See supra* Part I.B.

System access controls prevent unauthorized users from getting into a system, and force authorized users to be security conscious.[131] System access controls start with identification and authentication.[132] This may be as simple as providing a username and password,[133] or it may require technological devices to login, such as an electronic key, token, badge or smart card.[134] Some systems are so advanced that biometric or behavioral information is required to access them, such as fingerprints, handprints, retina pattern, iris pattern, voice, signature or keystroke patterns.[135] Other system access controls include transmission encryption,[136] challenge and response procedures,[137] and password controls.[138]

Data access controls are similar to system access controls, except that instead of protecting the system at-large, their protection is aimed at the data and programs inside the

[131] LEHTINEN ET AL., *supra* note 37, at 49.

[132] Identification is the way you tell the system who you are. Authentication is the way you prove to a system you are who you say you are. *Id.* at 50–51.

[133] *Id.* at 51.

[134] These devices contain electronic code that allows you to access a system, and may even be so sophisticated as to continually calculate new passwords based on time-of-day or secure algorithms. The computer system being accessed will have matching information to the security device, and will grant access once the petitioning party's password matches. *Id.*

[135] *Id.*

[136] LEHTINEN ET AL., *supra* note 37, at 52. Encryption scrambles data during transmission, which can only be unlocked with the correct session key. There are numerous encryption protocols that can be used, such as DES, Kerberos and Rijndael, all of which use some version of session keys to authenticate messages and protect communications. *See* LEHTINEN ET AL., *supra* note 37, at 137–72; COLARIK, *supra* note 6, at 72–73.

[137] Challenge and response is when users are asked to re-authenticate themselves frequently at random intervals throughout their session with the system. LEHTINEN ET AL., *supra* note 37, at 52.

[138] Password controls may attempt to stop unauthorized users from accessing a system. These controls can range from warning messages to unauthorized users, to limiting the number of attempts to enter the correct password, to implementing login failure wait times between attempts, to password locks for incorrect logins. Password controls may also force users to be more security conscious. These controls can range from forcing them to change their password at regular intervals, to requiring minimum length passwords, to showing users the date/time of their last login. *Id.* at 59–60.

system.[139] Authorization is the key to data access controls. It checks to see if the users of a system have rights to access particular files.[140] Data access controls allow multiple users to use a system without having to grant everyone access to every file on the system.[141] Other data access controls include data storage encryption,[142] and reference monitors.[143]

Security administration is the human side of computer security.[144] It uses security procedures to protect a system, delineates system administrator responsibilities, ensures users are trained on computer security, and monitors users to ensure security policies are observed.[145] Examples of security administration are setting and publicizing security policies,[146] performing risk analysis and disaster planning,[147] training and monitoring employees,[148] creating and maintaining user security profiles,[149] penetration testing,[150]

[139] *Id.* at 50.

[140] Systems typically maintain a file containing information about user privileges and characteristics. This is often called a security profile. *Id.* at 61–62.

[141] *See* LEHTINEN ET AL., *supra* note 37, at 61–67; COLARIK, *supra* note 6, at 69–71. This is another important layer of security on top of system access controls, as it helps stop attackers from accessing sensitive data/ programs after they've gained unauthorized access to a system. LEHTINEN ET AL., *supra* note 37, at 66.

[142] Encryption of stored data helps prevent the access of and tampering with sensitive information. COLARIK, *supra* note 6, at 71.

[143] Reference monitors review access attempts and cross-reference them against user security profiles. If a user attempts to access files above their access level, then the reference monitor alerts the system administrator. *Id.*

[144] LEHTINEN ET AL., *supra* note 37, at 96.

[145] *Id.* at 50.

[146] Security policies are designed to make systems more secure. An example of a security policy is the separation of administrator duties. The separation of duties prevents any one user from controlling the system's security mechanisms. By separating duties among a group of individuals, it becomes harder for cyberattackers to take control of a system through the impersonation of an individual account. *Id.* at 97, 108–10.

[147] *Id.* at 97.

[148] *Id.*

[149] LEHTINEN ET AL., *supra* note 37, at 97.

backing up system files,[151] arranging for the use of other computer facilities or equipment in case of an emergency,[152] and performing security audits.[153]

Secure system design uses hardware and software to protect the system.[154] Examples of security hardware are segmented system memory,[155] physical gateways,[156] and building a system to withstand denial-of-service attacks.[157] Examples of security software are anti-virus programs,[158] encryption programs, firewalls,[159] and intrusion detection systems.[160]

[150] Penetration testing is when the system administrator simulates cyberattacks to test a computer system for security holes. *Id.* at 97, 107–08.

[151] Backing up data may occur on site or at remote secure facilities, and is one of the most important things a system administrator can do to enable a compromised system to recover from a cyberattack. *Id.* at 96, 102.

[152] Backup systems may be essential in case a cyberattack cripples an organization's primary systems. *Id.* at 96.

[153] Security audits review user profiles and activity within a system, and look for suspicious account settings or activity. An effective component of a security audit is to review audit logs/trails. Audit logs/trails are designed to record activities and events within a computer system. Reviewing audit logs can reveal security breaches inside a system, and help trace the attacks back to their source. For instance, an audit log might contain information about the origin of a computer transmission, show which files were accessed or attempted to be accessed, and reveal changes to the computer system. LEHTINEN ET AL., *supra* note 37, at 108–09; COLARIK, *supra* note 6, at 71–72 (2006).

[154] LEHTINEN ET AL., *supra* note 37, at 50.

[155] Segmented system memory physically isolates privileged processes from non-privileged processes. *Id.*

[156] The easiest way to secure a computer network is to physically isolate it from the outside world. However, as systems become increasingly dependent on global communication to achieve their purpose, this becomes more difficult to do. There is a middle ground though. Systems can be physically designed so that communication to and from the system are routed through a single channel, known as a gateway. Gateways can be designed to run a variety of security programs, all aimed at ensuring that communication is coming from trusted sources for legitimate purposes. *Id.* at 189.

[157] This can include increasing bandwidth to handle the scope of the attack; building redundant or fault-tolerant systems that are harder to disrupt; or building the network so that it is easy to reconfigure in case of attack. *See id.* at 196.

[158] Anti-virus programs contain registries of virus code patterns, which can be used to detect viruses. Anti-virus programs lurk in the background of computer systems, constantly running and scanning ongoing processes and incoming data for viral code. Upon detecting a potential virus, it sounds an alarm and attempts to isolate/quarantine the dangerous code. *Id.* 92–93.

[159] "Firewalls protect computer systems by examining each packet of data that travels over the network. Clues about a packet's purpose can be read from its destination address. Firewalls contain a list of allowed and disallowed destinations and functions. If a packet is heading for a forbidden address or comes from one, the

Active defenses involve an in-kind response to a cyberattack, effectively a counter-cyberattack against the attacker's system, shutting down the attack before it can do further damage and/or damaging the perpetrator's system to stop it from launching future attacks.[161] Security professionals can setup active defenses to automatically respond to attacks against critical systems, or can carry them out manually.[162] For the most part, active defenses are classified, though programs that send destructive viruses back to the perpetrator's machine or packet-flood the intruder's machine have entered the public domain.[163] The specific capabilities that the government has developed are beyond the scope of this paper; however, it is essential to note that active defenses enhance victim-states' defensive capabilities against cyberattacks, providing states a crucial additional option over passive defenses alone.[164]

Defending against cyberattacks goes beyond computer security. On the macro level in the United States, "the federal government has taken steps to . . . encourage the private sector to also adopt stronger computer security policies and practices to reduce infrastructure

firewall stops it. If a packet is heading to a valid address, but its port identifier (the clue to the packet's function) is unknown or disallowed, the firewall stops that packet as well. Advanced firewalls even keep track of outgoing packets, and open up only if a packet is expected and returning." Firewalls help prevent active threats such as worms and viruses, which attempt to enter a computer via forbidden pathways. *Id.* 92.

[160] Intrusion detection systems monitor systems for attacks, much like anti-virus programs do for viruses. The intrusion detection systems have libraries of the steps that attackers typically take to conduct attacks. If an attack pattern is identified, it tries to stop the transaction (if it can) and places a call to the system administrator, informing them of the attempted attack. *Id.* at 107.

[161] *See* Jensen, *supra* note 26, at 231; Condron, *supra* note 25, at 410–11.

[162] *See* Jensen, *supra* note 26, at 231; David Wheeler & Gregory Larsen, *Techniques for Cyber Attack Attribution*, INST. DEF. ANALYSIS, Oct. 2003, at 23–24, *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859&Location=U2&doc=GetTRDoc.pdf.

[163] *See* Jensen, *supra* note 26, at 231; Condron, *supra* note 25, at 410–11.

[164] *See* Shachtman, *supra* note 26 (quoting the Air Force Research Laboratory as saying that passive defenses are insufficient to stop cyberattacks, and that active defenses are needed to mount an effective defense against cyberattacks); Crovitz, *supra* note 14, at 17 (arguing active defenses are needed to stop the cyberthreat).

vulnerabilities."[165] The National Strategy to Secure Cyberspace encourages the private sector to partner with federal agencies to improve computer security for U.S. critical infrastructure.[166] The National Cyber Security Division of the Department of Homeland Security is "tasked with conducting analysis of cyberspace threats and vulnerabilities, issuing alerts and warnings for cyberthreats, improving information sharing, responding to major cybersecurity incidents, and aiding in national-level recovery efforts."[167] Furthermore, the government has setup the Cyber Warning and Information Network and National Cyber Alert System, which is an early warning system for cyberattacks across the United States that coordinates national cybersecurity defenses across critical U.S. sectors.[168]

Unfortunately, computer security, in its present form, is not enough to stop cyberattacks. Computer software frequently has design flaws that open systems to attack, despite system administrators' best efforts to fully secure their computer systems.[169] These design flaws are compounded by administrator and user carelessness in both system design and use, which often nullify the security measures put in place to defend a system.[170] Furthermore, poor design of federal computer networks has left them with more entry points than U.S. early warning programs can effectively monitor at one time, leaving U.S. computer

[165] WILSON, *supra* note 15, at CRS-31.

[166] *Id.*

[167] *Id.*

[168] *Id.* at CRS-31 to CRS-32.

[169] *See id.* at CRS-24 to CRS-26.

[170] *See* LEHTINEN ET AL., *supra* note 37, at 96; WILSON, *supra* note 15, at CRS-25.

systems vulnerable to attack until the amount of entry points is reduced.[171] These vulnerabilities highlight the fact that passive defenses alone are not enough to protect states from cyberattacks. As a result, it is likely states will feel the need to use active defenses, and, in such event, it would be best if the law could provide parameters regarding the proper use of such active defenses.[172]

[171] *See* Ryan Naraine, *Chertoff Describes 'Manhattan Project' for Cyber Defenses*, EWEEK.COM, Apr. 8, 2008, http://www.eweek.com/c/a/Security/Chertoff-Describes-Manhattan-Project-for-Cyber-Defenses (referencing former Secretary of Homeland Security Michael Chertoff's speech on federal computer systems' vulnerability).

[172] Responding to cyberattacks with active defenses (a law of war response) is the only real way for states to protect themselves against cyberattacks. Given the inability of passive defenses to completely secure state CNI, states will look to the law to help prevent cyberattacks against them. The law can deal with cyberattacks in three different ways, as discussed below. However, as also discussed below, the two non-law of war methods for dealing with cyberattacks are inadequate.

First, states can continue to treat cyberattacks as a criminal matter. However, a number of states refuse to enforce their criminal laws when cyberattacks are directed at their rival states, or cooperate in international efforts to eliminate cyberattacks. These actions have made criminal laws insufficient to protect states from cyberattacks. *See* Creekman, *supra* note 25, at 656–63; *see also supra* Part I.B.

Second, states can try to use international treaties as a way to combat cyberattacks. These treaties could either regulate state responsibilities concerning international cyberattacks, or regulate the architecture and code used to build the internet. *See generally* Brown, *supra* note 52 (discussing the importance of an international convention on cyberattacks, and proposing a draft convention to regulate information systems in armed conflict); Hollis, *supra* note 23 (discussing the need for clear international laws for cyberspace); LESSIG, *supra* note 53 (arguing for a treaty to regulate the design of cyberspace that ensures digital identities are required for everything on the internet; this would make it easier for law enforcement to trace and prosecute cyberattacks). However, since meaningful international agreements require the agreement of a substantial majority of sovereign states on a common framework, it seems unlikely that any comprehensive treaty will be forthcoming in the near future. *See* LESSIG, *supra* note 53, at 298–324. Furthermore, it is naïve to think that a treaty will be a way to get states to cooperate, as states like China and Russia are already turning a blind eye to cyberattacks when it's convenient to them, despite international condemnation of the cyberattacks originating from them so far, and numerous United Nations General Assembly resolutions calling for cooperation against cyberattacks. *See supra* Part I.B (discussing China and Russia's unwillingness to cooperate with other states to investigate and prosecute attackers); *infra* Part V.C (discussing the U.N. General Assembly resolutions calling for international cooperation to eradicate cyberattacks).

Finally, states can try to figure a way around the legal crisis under the law of war, so that states can employ active defenses in addition to passive defenses. Of these options, finding a way to authorize active defenses under the law of war is the only real way to protect states from cyberattacks. This is because the first two options require state cooperation, which is not happening at present and seems unlikely to happen in the near future. Also, there is a good chance that a law of war response (using active defenses) will act as a coercive mechanism to push uncooperative states into changing their behavior, since no state wants another state operating within their borders, even electronically.

III. The General Framework of *Jus ad Bellum*

The law of war is divided into two principal areas, *jus ad bellum* and *jus in bello*.[173] *Jus ad bellum*, also known as the law of conflict management, is the legal regime governing the transition from peace to war.[174] *Jus in bello*, also known as the law of armed conflict, governs the actual use of force during war.[175] The analysis of cyberattacks predominantly falls under *jus ad bellum*, since *jus ad bellum* sets forth: (1) the thresholds that cyberattacks must cross to be considered a use of force, which then brings cyberattacks under the law of war, and (2) the legal options that states have to respond to cyberattacks.

Historically, the transition from peace to war fell under the prerogative of the sovereign; however, it came under the aegis of international law following World War II with the ratification of the United Nations (U.N.) Charter.[176] While the U.N. Charter is not the only source of *jus ad bellum*,[177] it has redefined and codified "contemporary *jus ad bellum* in its entirety" and has become the starting point for all *jus ad bellum* analysis.[178] The

[173] WINGFIELD, *supra* note 49, at 31.

[174] *Jus ad bellum* "is a set of rules that govern the resort to armed conflict and determine whether the conflict is lawful or unlawful in its inception." It governs what amounts to a use of force, and when force is authorized. *Id.* at 31, 33.

[175] *Jus in bello* "governs the behavior of both belligerents and neutrals during hostilities." It governs what types of force are authorized, and places limits on the use of force. *Id.* at 131.

[176] *Id.* at 31.

[177] *See* Hollis, *supra* note 23, at 1039 (noting that jus ad bellum comes from diverse sources, including the U.N. Charter, international humanitarian law treaties, and CIL).

[178] WINGFIELD, *supra* note 49, at 31, 37–38.

relevant articles of the U.N. Charter are Articles 2(4), 39 and 51, which provide the framework for modern *jus ad bellum* analysis.[179]

A. General Prohibition on the Use of Force

Article 2(4) prohibits states from employing "the threat or use of force against the territorial integrity or political independence of [another] state, or in any other manner inconsistent with the Purposes of the United Nations."[180] Sometimes known as *jus contra bellum*,[181] Article 2(4) criminalizes both the aggressive use of force and the threat of the aggressive use of force by states as crimes against international peace and security.[182] Although the U.N. Charter is a treaty and its protections apply to those states that are parties to the treaty, the prohibitions contained in Article 2(4) have come to be recognized as CIL as well, binding on all states across the globe.[183]

On its face, Article 2(4) might suggest that the threat or use force is only prohibited when directed against the territorial integrity or political independence of another state.[184] This is not the case.[185] Article 2(4) also prohibits any threat or use of force inconsistent with

[179] *Id.* at 31, 37–40.

[180] U.N. CHARTER art. 2(4).

[181] *Jus contra bellum* means the law against the aggressive use of force. WINGFIELD, *supra* note 49, at 38.

[182] *Id.* at 31, 38–39.

[183] Schmitt, *supra* note 58, at 521. Unlike treaty based law, which only binds parties to the treaty, CIL binds all states to it. CIL is formed when state practice matures to the point that it evidences *opinio juris sive necessitates*, a belief on the part of states that engaging in that practice is legally obligatory. *Id.* at 524. *See infra* notes 389–90 and accompanying text (discussing the formation of CIL in depth).

[184] *Id.* at 521–22.

[185] *Id.*

the purpose of the United Nations.[186] When read in conjunction with Article 1 of the U.N. Charter, Article 2(4) forbids threats or uses of force which threaten international peace and security.[187] Thus, states may not threaten to use or actually use force against another state unless an exception is carved out within the U.N. Charter.[188] This position is further supported by Article 2(3), which requires states to "settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered."[189] Only two exceptions exist to this seemingly all-encompassing renunciation on the use of force:[190] actions authorized by the U.N. Security Council[191] and self-defense.[192]

B. Actions Authorized by the United Nations Security Council

The first exception to the general prohibition on the use of force is actions authorized by the United Nations Security Council. This coercive authority stems from Article 42 of the U.N. Charter, which allows the Security Council to use military force to restore international

[186] U.N. CHARTER art. 2(4).

[187] *See* U.N. CHARTER art. 1 (stating that the purpose of the United Nations is to maintain international peace and security); Schmitt, *supra* note 58, at 522.

[188] YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 87–88 (4th ed. 2005).

[189] U.N. CHARTER art. 2(3).

[190] Jensen, *supra* note 26, at 216.

[191] *See* U.N. CHARTER art. 39 (stating that the Security Council shall decide what constitutes a threat to international peace and security, and what measures to take in response to any such threat); U.N. Charter art. 42 (granting the Security Council the power to use military measures to restore international peace and security).

[192] *See* U.N. CHARTER art. 51 (re-affirming the inherent right of states to use force in self-defense under CIL).

peace and security.[193] However, while the U.N. Charter grants the Security Council power to use military force, it cannot do so until it has met certain conditions, which are laid out in Articles 39, 41 and 42.[194]

Article 39 is the first threshold that the Security Council must cross before it can authorize the use of force.[195] The Security Council must consider whether a "threat to the peace, breach of the peace, or act of aggression" exists.[196] Should the Security Council determine that this threshold has been met, in essence determining that a state has violated its obligations under Article 2(4), the Security Council may then move on to Articles 41 and 42, to determine the appropriate course of action to restore international peace and security.[197]

Article 41, the use of non-military measures, is the Charter's preferred method for restoring international peace and security.[198] Under it, the Security Council may authorize non-military measures to coerce an offending state into ceasing its aggression.[199] The non-military measures are implemented by member states of the United Nations and may include

[193] U.N. CHARTER art 42.

[194] WINGFIELD, *supra* note 49, at 31, 52–54.

[195] *See* Schmitt, *supra* note 58, at 525.

[196] *Id.* (quoting Article 39 of the U.N. Charter).

[197] *See* WINGFIELD, *supra* note 49, at 52–54. Remember, states are generally prohibited from threatening to use or using force, and are required to seek peaceful means to resolve their disputes with each other. *See* U.N. CHARTER arts. 2(3), 2(4). Fortunately, the drafters of the Charter understood that some states would not live up to these requirements and created a framework to deal with them. "As an exercise of the international community's inherent right of collective self-defense, Article 39 of the Charter imposes an obligation on the Security Council to maintain international peace and security." WINGFIELD, *supra* note 49, at 52. From this obligation, and through the mechanisms prescribed by Articles 41 and 42, the Security Council derives the power to authorize the force against states who threaten the peace. *Id.* at 52–54.

[198] *See* Schmitt, *supra* note 58, at 525.

[199] *See id.*

the "complete interruption of economic relations . . . and other means of communication, and the severance of diplomatic relations."[200]

Article 42, the use of military measures, like Article 41, requires an Article 39 threshold decision to be made, and only then used after non-military measures have proven unsuccessful, or after the Security Council determines that it would be fruitless to adopt them.[201] However, unlike its Article 41 powers, the Security Council may only authorize member states to take military action; it cannot compel them to do so.[202]

C. Self-Defense

The second exception to the general prohibition on the use of force is self-defense. This defensive right of states is enshrined in Article 51 of the U.N. Charter, which proclaims that "nothing in the present Charter shall impair the inherent right of [states to engage in] individual or collective self-defense" in response to an "armed attack."[203] As the text of Article 51 implies, the right of self-defense existed long before the U.N. Charter, and has

[200] U.N. CHARTER art. 41. Article 41 explicitly recognizes the Security Council's authority to give orders to member states. WINGFIELD, *supra* note 49, at 53–54. "The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter." U.N. CHARTER art. 25.

[201] *See* U.N. CHARTER art. 42; Schmitt, *supra* note 58, at 525.

[202] WINGFIELD, *supra* note 49, at 54. When the Security Council authorizes the use of force against a state under Article 42, its authorizing resolution serves as legal authority. The Security Council can authorize states to use military force in three different ways. First, it can authorize states to use force to enforce its resolution. Second, it can authorize international organizations, such as NATO, to use force on its behalf. Third, it can create a U.N. military force and ask states to provide military forces to it. In all of the cases, state participation is strictly voluntary and cannot be compelled. SCHMITT, *supra* note 58, at 525–28.

[203] U.N. CHARTER art.51. Article 51 only allows states to act in self-defense until the Security Council takes action to restore international peace and security. Furthermore, states are required to immediately report measures taken in self-defense to the Security Council. U.N. CHARTER art.51; DINSTEIN, *supra* note 188, at 177 (quoting Article 51 of the U.N. Charter).

been re-affirmed in the Charter as an inherent right of states under CIL.[204] Self-defense is derived from the fundamental right of states to survive, allowing them the self-help measure of using force defensively to protect themselves and their citizens.[205] Since this right exists independent of and has not been subsumed by the U.N. Charter,[206] self-defense analysis draws on both the provisions of Article 51 of the U.N. Charter and the principles of CIL.[207]

The bedrock principle of self-defense is that it may be invoked in response to an armed attack.[208] Unfortunately, while this cornerstone is universally recognized under international law, ambiguity in the U.N. Charter has led to an ongoing debate about when states may invoke self-defense.[209] This is because the Charter never defines "armed attack."[210] Since the timing of self-defense is contingent on an armed attack occurring, it is critical to resolve what constitutes an armed attack.[211] This debate has become even more pronounced regarding cyberattacks, which are often seen as a use of force short of armed

[204] *See* DINSTEIN, *supra* note 188, at 175–82.

[205] *Id.* at 175–76.

[206] *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 94, 96–97 (June 27) (noting that the inherent right of self-defense has not been subsumed by the U.N. Charter); DINSTEIN, *supra* note 188, at 181 (citing the International Court of Justice's (ICJ) opinion in the *Nicaragua* case); Jensen, *supra* note 26, at 221 (citing the ICJ's opinion in the *Nicaragua* case). *But see* WINGFIELD, *supra* note 49, at 41 (citing THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 666 (Bruce Simma ed. 1994), which concludes that Article 51 excludes any right of self-defense "other than that in response to an armed attack").

[207] *See* DINSTEIN, *supra* note 188, at 181; WINGFIELD, *supra* note 49, at 41 (noting that the Article 51 right of self-defense is coextensive with the right of self defense under CIL).

[208] U.N. CHARTER art. 51.

[209] Hollis, *supra* note 23, at 1040–41.

[210] *See* WINGFIELD, *supra* note 49, at 73; Hollis, *supra* note 23, at 1040–41.

[211] *See* WINGFIELD, *supra* note 49, at 41 (noting that the pivotal focal point in any self-defense debate is the meaning of an armed attack, since that will determine the time that an armed attack occurs and when self-defense may be invoked); Jensen, *supra* note 26, at 219–20.

force, making cyberattacks far more difficult to classify than traditional attacks with conventional weapons.[212]

Self-defense analysis is further complicated because of competing theories among legal scholars on the interplay between the U.N. Charter and CIL.[213] Some commentators place heavier emphasis on the U.N. Charter, arguing that Article 51 limits self-defense to responses against actual armed attacks.[214] Others place more emphasis on CIL, arguing for a broader interpretation of armed attacks that includes imminent armed attacks.[215] Imminent armed attacks are addressed in Part III, Section D. For now, remember that while there are different theories about the definition of an armed attack, once a state is targeted with an armed attack, the state and its allies are legally authorized to use force against the aggressor.

Self-defense responses must comply with international law. Just because an armed attack has occurred against a victim-state, does not mean that the victim-state has a blank check to wage unlimited war against an aggressor.[216] Self-defense must comply with two principles of CIL—necessity and proportionality.[217] Necessity is the requirement that self-

[212] *See infra* Part V.A (addressing the question of whether a cyberattack constitutes an armed attack).

[213] *See* WINGFIELD, *supra* note 49, at 46–47 (noting the different opinions legal scholars have on the interplay between Article 51 and CIL regarding anticipatory self-defense); Murphy, *supra* note 50, at 705 (noting the lack of consensus on the legality of anticipatory self-defense due to competing views on the interplay between the U.N. Charter and CIL).

[214] *See* Jensen, *supra* note 26, at 219–20; Barkham, *supra* note 30, at 74; Murphy, *supra* note 50, at 706–11 (discussing the strict-constructionist school of thought on the U.N. Charter and armed attacks).

[215] *See* Jensen, *supra* note 26, at 221–26; Barkham, *supra* note 30, at 74–75; Murphy, *supra* note 50, at 706–11 (discussing the imminent threat and qualitative threat schools of thought on CIL and armed attacks).

[216] *See* DINSTEIN, *supra* note 188, at 235–37.

[217] WINGFIELD, *supra* note 49, at 41–44. *But see* DINSTEIN, *supra* note 188, at 237, 242–43(noting that self-defense must comply with three principles of CIL—necessity, proportionality and immediacy; under this analysis immediacy means that self-defense measures cannot be delayed indefinitely and must be taken in a reasonable amount of time after an armed attack).

defense is actually required under the circumstances because a reasonable settlement could not be attained through peaceful means.[218] Therefore, a state that is subject to an all-out invasion will, no doubt, be required to use force to overcome the aggressor; whereas a state that is subject to an isolated border skirmish might not need to use force to protect itself.[219] Proportionality requires self-defense actions to be limited to the amount of force necessary to defeat an ongoing attack or deter future aggression.[220] It is important to understand that this principle does not require the size and scope of defensive actions to be similar to those of the attack. A defensive action may need to employ significantly greater force than the attacker used to successfully repel the attacker.[221] The key is to determine the amount of force needed to either defeat the current attack or deter future attacks from occurring. For instance, after an all-out invasion, a proportionate response might entail an all-out war to defeat the aggressor's military, including the use of nuclear weapons, since that may be the only feasible way to deter future attacks.[222] On the other hand, a proportionate response to an isolated missile strike might be to strike the launching facility for that missile.[223] These principles define the scope of self-defense responses, and provide insight into the rationale behind when self-defense is required.

The principle of immediacy originated in relation to anticipatory self-defense, and, for the most part, is accepted as a third principle which only applies to anticipatory self-defense. *See infra* Part III.D.

[218] DINSTEIN, *supra* note 188, at 237.

[219] *Id.*

[220] *See* Schmitt, *supra* note 58, at 532.

[221] *See id.*

[222] *See* DINSTEIN, *supra* note 188, at 237–42.

[223] *See* WINGFIELD, *supra* note 49, at 48.

D. Anticipatory Self-Defense

Anticipatory self-defense is a subset of self-defense.[224] Its basis is that "aggression often begins without shots being fired or borders being crossed."[225] Sometimes states will obtain information which reveals that an armed attack is about to be launched against them. While the attack hasn't yet occurred, "states can rightfully defend themselves against such violence."[226]

> The crux of the issue, therefore, is not who fired the first shot but who embarked upon an irreversible course of action, thereby crossing the legal Rubicon. The casting of the die, rather than the actual opening of fire, is what starts the armed attack. It would be absurd to require that the defending State should sustain and absorb a devastating (perhaps a fatal) blow, only to prove the immaculate conception of self-defense.[227]

Anticipatory self-defense is a long-standing tenet of CIL, dating back to the 1836 *Caroline* case.[228] In *Caroline*, the United Kingdom and the United States agreed that self-defense was lawful in advance of an armed attack, when "the necessity of that self-defense is instant, overwhelming and leaving no choice of means, and no moment for deliberation."[229]

[224] MICHAEL WALZER, JUST AND UNJUST WARS 74 (1977); *see also* Murphy, *supra* note 50, at 706–11 (noting students of the imminent threat and qualitative threat schools of thought on CIL treat imminent armed attacks as armed attacks for purposes of self-defense). *But see* Murphy, *supra* note 50, at 706–11 (noting some legal scholars strictly construe the U.N. Charter to authorize self-defense only in response to actual armed attacks).

[225] *Id.*

[226] *Id.*

[227] DINSTEIN, *supra* note 188, at 191. Dinstein calls this interceptive self-defense, arguing that armed attacks should be more broadly construed than invasive force across national borders; however, his justification for interceptive self-defense is the same justification for anticipatory self-defense. The only real distinction between the Dinstein and other legal scholars is the timing of anticipatory self-defense, which shall be addressed in this section. Barkham, *supra* note 30, at 76–77.

[228] *See* Barkham, *supra* note 30, at 75; Murphy, *supra* note 50, at 705.

[229] WINGFIELD, *supra* note 49, at 47 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 675 (Bruno Simma ed. 1994) (quoting then Secretary of State Daniel Webster)).

As discussed in Part III, Section C, anticipatory self-defense is not a universally accepted principle among legal scholars;[230] however, despite ongoing debate, stronger arguments exist in support of anticipatory self-defense as a fundamental axiom of international law.[231] The real question then becomes when states can act in anticipatory self-defense.

[230] *See supra* Part III.C.

[231] International law is derived from four sources: international conventions, international custom (as evidence of a general principle accepted as law), the general principles of law recognized by civilized nations, and the judicial decisions and the teachings of the most highly qualified international legal scholars (as a subsidiary means for determining the rules of law). *See* WINGFIELD, *supra* note 49, at 72 (quoting Statute of the International Court of Justice, art. 38(1), June 26, 1945, 59. Stat. 1055, 1060 (1945)).

With regard to international conventions, the text of the U.N. Charter states that it does nothing to impair the inherent right of self-defense. Even more persuasive may be the fact that the French language version of the Charter, which is equally as authoritative as the English version, preserves the inherent right of nations to act in self-defense in situations where *the member-state is the object of an armed aggression*. This is a much less restrictive version, which supports the fact that the drafters intended to preserve the right of self-defense as it existed prior to the Charter. *See* Murphy, *supra* note 50, at 706–15.

With regard to international custom, there are numerous instances of states justifying their actions based on anticipatory self-defense post-United Nations Charter. Examples include, the 1962 quarantine of Cuba by the United States, the 1967 Arab-Israeli war, the 1981 Israeli attack against an Iraqi nuclear facility, and the 1986 U.S. bombing against Libya. *See* Murphy, *supra* note 50, at 713; Thomas Franck, *When, If Ever, May States Deploy Military Force Without Prior Security Council Authorization?*, 5 WASH. U. J.L. & POL'Y 51, 59 (2001).

With regard to judicial decisions, the ICJ stated that self-defense was not subsumed by the U.N. Charter. The court also left the door open to anticipatory self-defense as a valid axiom of international law, but chose not to resolve the issue since the parties in the case had not raised it. *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 110 (June 27); DINSTEIN, *supra* note 188, at 181 (citing the ICJ's opinion in *Nicaragua*); Jensen, *supra* note 26, at 221 (citing the ICJ's opinion in *Nicaragua*).

With regard to legal scholarship, respected scholars seem to support anticipatory self-defense as a maxim of international law. *See* WALZER, *supra* note 224, at 82–85 (recognizing the Six Day War as a lawful use of force by Israel in anticipation of an imminent armed attack); DINSTEIN, *supra* note 188, at 191 (rejecting the doctrine of anticipatory self-defense, but recognizing the right of interceptive self-defense before an attack occurs); WINGFIELD, *supra* note 49, at 47, 94 (recognizing the right of states to act in anticipatory self-defense, and noting that even opponents of anticipatory self-defense concede that self-defense may begin after an attack is launched, but before it occurs); Murphy, *supra* note 50, at 706–15 (noting that even strict-constructionists admit that self-defense may be justified on moral or political grounds); Barkham, *supra* note 30, at 75 (noting that even staunch opponents of anticipatory self-defense allow some leeway on interpreting when an attack begins and admits that technology may require states to re-examine the starting point of armed attacks); Schmitt, *supra* note 58, at 528–36 (recognizing anticipatory self-defense as a valid subset of self-defense).

The timing of anticipatory self-defense actions depends on the imminency of an attack.[232] Imminency, sometimes called immediacy and sometimes referred to as the third principle of self-defense, supplements the traditional self-defense principles of necessity and proportionality regarding anticipations.[233] Generally speaking, imminency allows a state to use force against an identified aggressor, in advance of an armed attack, to repel the attack before it is launched.[234] Initially, the concept of imminency restricted anticipatory self-defense to situations immediately before an attack, where an attack had been detected and there was no time to deliberate about other means of preventing the attack short of forceful self-defense.[235] The principle effectively balanced the victim-state's right to ward off violence against its international obligation to find peaceful means to resolve disputes.[236] However, due to changes in the nature of warfare, imminency has evolved significantly since then.[237] Today, imminency allows states to legally employ force in advance of an attack, at the point when (1) evidence shows that an aggressor has committed itself to an armed attack, and (2) delaying a response would hinder the defender's ability to mount a meaningful defense.[238] Thus, imminency is actually a relative concept,[239] which operates as follows:

[232] *See* Schmitt, *supra* note 58, at 528–36.

[233] *See id.* at 533.

[234] *See id.* at 533–34.

[235] *See id.* (recalling the standards set forth in the *Caroline* case).

[236] *See id.* at 534.

[237] *See id.* (noting that it's become accepted to invoke anticipatory self-defense earlier and earlier, in advance of an attack, as the consequences of a single attack become more severe (in the case of chemical, biological or nuclear weapons) and as intelligence gathering tools become more advanced (satellite imagery, intercepted electronic communications and other state-of-the-art surveillance techniques)).

[238] *See id.* at 534–35.

> Weak states may lawfully act sooner than strong ones in the face of identical threats because they are at a greater risk as time passes. In the same vein, it may be necessary to conduct defensive operations against a terrorist group long before a planned attack because there is unlikely to be another opportunity to target terrorists before they strike. . . . In other words, each situation presents a case-specific window of opportunity within which a State can foil an impending attack.[240]

Finally, one should note just because a single attack may be finished, doesn't mean that future attacks are not imminent. When evidence suggests that an attack is part of an ongoing campaign against a state, such as the terrorist attacks against the United States on 9/11, future armed attacks will be considered imminent and anticipatory self-defense will be authorized.[241] Some scholars support the same conclusion, but disagree with the legal rationale behind it, claiming that a proportional response in self-defense to a single armed attack can be far reaching to deter future attacks, and that anticipatory self-defense is the wrong lens through which to view the response to an ongoing campaign.[242]

E. Proportionate Countermeasures / Reprisals

Proportionate countermeasures, also known as reprisals, provide another way for states to address illegal uses of force against them.[243] As discussed in Part III, Section C, no consensus exists as to what constitutes an armed attack, which creates the possibility that a

[239] *See id.* at 534.

[240] *Id.*

[241] *See id.* at 535–36.

[242] *See* Murphy, *supra* note 50, at 734–36 (arguing that self-defense allowed the United States to conduct a far reaching campaign against Al Qaeda in response to the 9/11 attacks on the grounds of self-defense, not anticipatory self-defense).

[243] *See* WINGFIELD, *supra* note 49, at 85; Jensen, *supra* note 26, at 220.

cyberattack may be seen as a use of force below the armed attack threshold.[244] As a result, it is important to explore the rights that states have to react to illegal uses of force against them which fall short of an armed attack.

Proportionate countermeasures are an exception to the general rule that states are required to solve their disputes peacefully.[245] "A reprisal 'is an act which is unlawful *per se*, unless it can be justified as a countermeasure triggered by an unlawful act and is designed to induce the offending state to return to full compliance with the law.'"[246] Should a state decide to use proportionate countermeasures, it must comply with the three criteria enumerated by the International Court of Justice (ICJ) in *Nicaragua*.[247] These criteria are:

> First, the action must be taken in response to a previous international wrong act of another state, and it must be directed against that state. Second, the injured state must have called upon the offending state to discontinue its wrongful conduct or to make reparation for it. Third, the countermeasures must be commensurate with the injury suffered, taking into account the rights in question.[248]

Reprisals may be carried out in various ways. Economic and political coercion are the two main forms of reprisals; however, reprisals could also include the use of limited cyberattacks against an aggressor.[249] The limits on reprisals are that they may not involve the use of force contrary to Article 2(4) of the U.N. Charter;[250] however, the consensus

[244] *See supra* Part III.C.

[245] *See* WINGFIELD, *supra* note 49, at 84–85.

[246] *See id.* at 85 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 101 (Bruno Simma ed. 1994)).

[247] Jensen, *supra* note 26, at 220.

[248] *Id.*

[249] *See* WINGFIELD, *supra* note 49, at 84–92.

[250] *See id.* at 85.

amongst international scholars is that this prohibition really only amounts to a prohibition against armed force.[251] While this paper contends that states should treat certain cyberattacks as armed attacks, and deal with them using self-defense and anticipatory self-defense legal principles, reprisals provide an important alternate theory for dealing with cyberattacks to those who contend that cyberattacks fall short of the armed attack threshold.[252]

The general framework of *jus ad bellum* discussed so far has primarily evolved in response to state-on-state attacks. When attacks are carried out by non-state actors across state borders, it complicates the framework governing state responses to the attacks. Since most cyberattacks are carried out by non-state actors, this paper will explore *jus ad bellum* in greater depth and explain the intricacies of state responses to attacks by non-state actors.

IV. Non-State Actors Complicate the General Framework of *Jus ad Bellum*; However, Imputing State Responsibility Allows States to Deal with Them

International cyberattacks by non-state actors complicate the general framework of *jus ad bellum*. Since the prevailing view of international law requires states to attribute an attack to a state or its agents before responding with force,[253] states feel obligated to undertake lengthy, time-consuming investigations before responding to cyberattacks, which increases the risks that the cyberattack poses to them.[254] This creates a dilemma for states.

[251] *See id.* at 87 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 112 (Bruno Simma ed. 1994)).

[252] *See infra* Part V.A (discussing cyberattacks as armed attacks).

[253] *See* Condron, *supra* note 25, at 415; Dinstein, *supra* note 188, at 111.

[254] *See* Condron, *supra* note 25, at 407–08.

While states can trace an attack back to a server in another state, identifying who is at the other end of the electronic connection directing the attack takes more time than states have to make a decision about how to respond to the attack. Thus, under the prevailing view, states must guess whether the attacks were committed by a state or its agents, in which case the attacks would fall under the aegis of the law of war,[255] or by a non-state actor, in which case the attacks would fall under host-state criminal laws.[256] Thus, the prevailing view of the law forces states into a response crisis during an international cyberattack.[257]

Unfortunately, a lack of state cooperation has exacerbated the response crisis.[258] In an ideal world, states would not commit cyberattacks and would assist victim-states to track down their attackers. Under this utopian paradigm, states could contently rely on passive defenses, knowing that attackers who breached their defenses would be hunted down and punished under host-state criminal laws. Unfortunately, this is not a reality, and states are left in limbo following a cyberattack, wondering who attacked them, but how to respond. Yet even if a cyberattack was attributable to a non-state actor and states wanted to respond with force, they are bound not to intervene in the domestic affairs of other states.[259] Not surprisingly, despite a lack of state cooperation, states attempt to respond via host-state criminal law, rather than risk unlawfully violating the sovereignty of another state.[260]

[255] *See id.* at 414.

[256] *See id.* at 414–15.

[257] *See supra* Part I.B (discussing the response crisis).

[258] *See id.* (discussing the lack of state cooperation in tracking down attackers).

[259] Hollis, *supra* note 23, at 1049–50. To do so would be a violation of the sovereignty of the other state, and would be in violation of CIL. *Id.*

[260] *See supra* Part I.B.

There is, however, a way to avoid the attribution problem and response crisis. If a victim-state could lawfully impute a cyberattack to its state of origin and the state origin is unwilling to rectify the problem, it could immediately respond with force under the law of war, regardless of whether the attack was conducted by the state itself or by non-state actors within it.[261] Thus, imputing state responsibility creates a legal path for states to respond to cyberattacks with active defenses in a timely and effective manner. Given the technological and diplomatic limitations to timely attack attribution,[262] it is crucial for legal scholars to reexamine the legal regime governing state responses to cyberattacks through the lens of imputed responsibility.

The legal analysis for determining whether cyberattacks by non-state actors can be imputed to their state of origin starts with the underlying law behind armed attacks by non-state actors. From there, the analysis continues with the duties states have to one another concerning non-state actors within their territory, then moves on to the ways to impute state responsibility for acts by non-state actors, and ends with the legality of cross-border operations against other states. This part examines those issues, and afterwards, Part V analyzes cyberattacks under the framework established in Parts III and IV.

A. Armed Attacks by Non-State Actors

[261] *See infra* Part V.B–C.

[262] *See supra* Part I.B (discussing the attribution problem).

Non-state actors can and have committed armed attacks against states.[263] Most legal scholars believe these attacks fall under the aegis of the law of war.[264] Their opinion enjoys broad support from all four sources of international law: international conventions, international custom (as evidence of a general principle accepted as law), the general principles of law recognized by civilized nations, and the judicial decisions and teachings of the most highly qualified international legal scholars (as a subsidiary means for determining the rules of law).[265] However, since this opinion is not universally held,[266] it is worth discussing this at some length.

Of the four sources of international law, international treaties lend the least support for this proposition. This is because their support is, at best, indirect, stemming from their silence on the subject. Their silence allows states to infer support for this proposition because no treaty has ever prohibited states from treating attacks by non-state actors as acts of war, despite the opportunity to do so. As noted earlier, modern *jus ad bellum* analysis starts with the U.N. Charter.[267] Unfortunately, the Charter was written to govern armed

[263] *See* DINSTEIN, *supra* note 188, at 187, 204; WALZER, *supra* note 224, at 197–206 (discussing various terrorist campaigns); Schmitt, *supra* note 58, at 536–40 (discussing the Sept. 11, 2001 terrorist attacks by Al Qaeda).

[264] *See* DINSTEIN, *supra* note 188, at 204–08; Michael Schmitt, *Counter-Terrorism and the Use of Force in International Law*, *in* INTERNATIONAL LAW AND THE WAR ON TERROR 7, 33–47 (Fred L. Borch & Paul S. Wilson eds., Naval War College 2003); Schmitt, *supra* note 58, at 536–40; Rein Mullerson, *Jus Ad Bellum and International Terrorism*, *in* INTERNATIONAL LAW AND THE WAR ON TERROR 75, 106–11 (Fred L. Borch & Paul S. Wilson eds., Naval War College 2003).

[265] *See* WINGFIELD, *supra* note 49, at 72 (quoting Statute of the International Court of Justice, art. 38(1), June 26, 1945, 59. Stat. 1055, 1060 (1945)).

[266] Some scholars argue that the law of war only governs attacks by states. Schmitt, *supra* note 58, at 536.

[267] *See supra* Part III, introduction.

conflict between states.[268] As a result, the Charter is silent about armed attacks by non-state actors.[269] While it appears that the minimalist language of Article 51 allows a state to respond in self-defense to armed attacks against it,[270] the lack of any specific language on point forces us to look to the other three sources of international law to determine the controlling standards for armed attacks by non-state actors.

While not originally envisioned in the drafting of the U.N. Charter, analysis of CIL reveals that "[i]t is now incontrovertible that States treat the law of self-defense as applicable to acts by non-state actors."[271] The international community's response to the terrorist attacks of September 11, 2001 (9/11) crystallized the validity of this principle.[272] Following the 9/11 attacks, the U.N. Security Council passed Resolution 1368, which characterized the attacks as a threat to international peace and security under Article 39 of the Charter and reaffirmed the United States' inherent right to engage in either individual or collective self-

[268] *See* U.N. CHARTER art. 1 (stating that its purpose is to maintain international peace and security through the regulation of state action); Schmitt, *supra* note 58, at 536 (noting that the U.N. Charter was drafted to regulate state-on-state armed conflicts); Mullerson, *supra* note 264, at 112 (stating that there is little doubt that the drafters of the Charter had not contemplated armed attacks by non-state actors).

[269] *See generally* U.N. CHARTER (making no mention of non-state actors anywhere in the Charter).

[270] DINSTEIN, *supra* note 188, at 204 (noting that Article 51 regulates state responses to armed attacks, but never specifies the character of the perpetrator of the attacks; therefore implying that self-defense could be invoked against states or non-state actors); Schmitt, *supra* note 264, at 33–34 (noting that Chapter VII of the Charter, which includes both Articles 39 and 51, dictates what states may do in the face of threats to international peace and security and acts of aggression, without ever stating what those might be). *But see* Schmitt, *supra* note 58, at 536 (noting a number of commentators assert that because the U.N. Charter does not specifically address armed attacks by non-state actors, those attacks therefore fall outside the scope of the law of war and should, instead, be governed by international and domestic criminal laws).

[271] Schmitt, *supra* note 58, at 539.

[272] *See* DINSTEIN, *supra* note 188, at 207–08; Schmitt, *supra* note 264, at 7–47; Schmitt, *supra* note 58, at 536–40; Mullerson, *supra* note 264, at 84, 106–19.

defense in accordance with Article 51 of the Charter.[273] Two weeks after the attacks, when it appeared clear that Al Qaeda was behind the attacks, the Security Council passed Resolution 1373, once again affirming the United States' inherent right of self-defense in response to the attacks.[274] Both of these Security Council declarations are particularly significant because the 9/11 attacks could have been dealt with under Article 42 of the Charter, but instead were dealt with under Article 51, despite the fact that the attacks were committed by non-state actors.[275] NATO, the Organization of American States, and Australia all made similar declarations, invoking the collective self-defense provisions of their treaties, to assist the United States in response to the 9/11 attacks.[276] The statements and actions of scores of other states, including major states such as Russia, China, India, Japan, South Korea, Pakistan, Saudi Arabia and Egypt, lend support to the principle that attacks by non-state actors fall under the law of war.[277] Finally, this principle is supported by the ICJ in its 2004 Advisory Opinion in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*,[278] as well as from the publications of legal scholars.[279]

[273] *See* Schmitt, *supra* note 58, at 536–37 (noting that at the time Resolution 1368 was passed, no one believed that a state was behind the attacks, yet the attacks were found to be a threat to international peace and security under Article 39).

[274] *See id.* at 537.

[275] *See* Schmitt, *supra* note 264, at 16. Had the Security Council wanted to deal with the 9/11 attacks under Article 42 of the U.N. Charter, it could have authorized the United States, a coalition of forces, or a regional organization to use force pursuant to it, "as the Council is entitled to do in the face of a 'threat to the peace, breach of peace or act of aggression.'" *Id.* (quoting Article 42 of the U.N. Charter).

[276] NATO unanimously invoked Article 5 of the Washington Treaty, based on Article 51 of the U.N. Charter, which provides for collective self-defense in response to armed attacks against a member-state. The Organization of American States invoked the collective self-defense provision of the Rio Treaty. Australia invoked Article IV of the ANZUS Treaty. *See id.* at 16–18.

[277] *See* Schmitt, *supra* note 264, at 18; Schmitt, *supra* note 58, at 538–39.

[278] *See* DINSTEIN, *supra* note 188, at 204 (referencing the Separate Opinions of Judge Higgins and Judge Kooijmans, as well as the Declaration of Judge Buergenthal, in *Legal Consequences of the Construction of a*

While attacks by non-state actors fall under the law of war, the law of war only allows states to forcibly respond to these attacks when the attacks are imputable to a state,[280] meaning the state also bears some responsibility for the actions of the non-state actors. The next step of the analysis toward imputing state responsibility for these attacks is, therefore, to examine the duties that states have concerning non-state actors within their territory.

B. Duties Between States

"It is a long established principle of international law that 'a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people.'"[281] This principle is reflected in numerous state declarations, judicial opinions and publications from leading scholars.[282] State declarations that support this principle include: the 1970 Declaration on Friendly Relations, which urges states to "refrain from . . . acquiescing [to] organized activities within [their] territory directed towards the

Wall in the Occupied Palestinian Territory, 2004, 43 I.L.M. 1009, 1063, 1072, 1079 (2004)). While the ICJ held that Israel could not respond in self-defense to terrorist attacks from non-state actors in this case, the court explicitly stated this was because Israel never asserted the acts were imputable to a state. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 2004, 43 I.L.M. 1009, 1050 (2004). Thus, the case shows that attacks by non-state actors fall under the law of war, but that the law of war only permits states to respond in self-defense when the actions of the non-state actors are imputable to a state, which wasn't the case here.

[279] *See* DINSTEIN, *supra* note 188, at 204–08; Schmitt, *supra* note 264, at 33–47; Schmitt, *supra* note 58, at 536–40; Mullerson, *supra* note 264, at 106–11.

[280] *See supra* note 278 and accompanying text; *infra* Part IV.C–D.

[281] Schmitt, *supra* note 58, at 540–41 (quoting John Basset Moore in S.S. Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 4, 88 (Moore, J., dissenting)).

[282] *See* DINSTEIN, *supra* note 188, at 205–06; Schmitt, *supra* note 264, at 39–40, 48; Schmitt, *supra* note 58, at 541.

commission of [civil strife or terrorism in another state];"[283] the 1994 Declaration on Measures to Eliminate Terrorism;[284] and the 1996 Declaration on the Strengthening of International Security, which stated that states "must refrain from organizing, instigating, assisting or participating in terrorist acts in territories of other States, or from acquiescing in or encouraging activities within their territories directed towards the commission of such acts."[285] Case law that supports this principle include: *Corfu Channel*, in which "the International Court of Justice pronounced that every state is under an obligation 'not to allow knowingly its territory to be used for acts contrary to the rights of other states;'"[286] and *Tehran*, in which the ICJ re-affirmed that states "are required under international law to take appropriate acts in order to protect the interests" of other states from non-state actors within their borders.[287] Finally, scholars have noted this principle "is so widely recognized that it should not fuel a debate."[288]

[283] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, ¶ 1, U.N. GAOR, 25th Sess., Annex, Agenda Item 85, U.N. Doc. A/Res/2625 (Oct. 24, 1970); *see also* Vincent-Joel Proulx, *Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?*, 23 BERKELEY J. INT'L L. 615, 629 (2005); Schmitt, *supra* note 264, at 39–40 (quoting the 1970 Declaration on Friendly Relations).

[284] Schmitt, *supra* note 264, at 40 (citing the 1994 Declaration on Measures to Eliminate International Terrorism, G.A. Res. 49/60, U.N. GAOR 6th Comm., 49th Sess., 84th plen. mtg., Annex, U.N. Doc. A/49/743 (1994)).

[285] *Id.* at 48 (quoting Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism, G.A. Res. 51/210, U.N. GAOR 6th Comm., 51st Sess., 88th plen. mtg., Annex, U.N. Doc. A/51/631 (1996)).

[286] DINSTEIN, *supra* note 188, at 205–06 (quoting Corfu Channel case (Merits), 1949 I.C.J. Rep. 4, 22 (Apr. 9)); *see also* Schmitt, *supra* note 264, at 49.

[287] DINSTEIN, *supra* note 188, at 206 (citing Case Concerning United States Diplomatic and Consular Staff in Tehran, 1980 I.C.J. Rep. 3, 32–33, 44 (May 24)).

[288] Proulx, *supra* note 283, at 629–60; *see also* DINSTEIN, *supra* note 188, at 205–06 (noting further support from Ian Brownlie, in addition to himself); Proulx, *supra* note 283, at 659–66 (noting further support from Davis Brown, Lee Feinstein, Matthew Lippman and Ann-Marie Slaughter); Schmitt, *supra* note 264, at 39–40, 48; Schmitt, *supra* note 58, at 540–41.

In short, it is clear from state practice and *opinio juris* that states have an affirmative duty to prevent non-state actors within their borders from committing armed attacks on other states.[289] Toleration of such attacks constitutes a crime under international law.[290] Thus, "a host-state that has the capability to prevent [an armed attack by non-state actors] but fails to do so will inherently fail to fulfill its duty" under international law.[291] However, it isn't realistic to expect states to completely prevent armed attacks by non-state actors from ever occurring.[292] As a result, the dispositive factor in evaluating whether states live up to their duty "will lie, rather, in the conduct of the host-state itself in addressing the potential threat and in attaining a realistic result in light of the factual circumstances."[293]

In and of itself, the duty to prevent attacks does not make states responsible for every cross-border attack by non-state actors that emanates from their territory. However, it does bridge the gap between the actions of non-state actors and state responsibility for those acts. The next section completes the analysis of imputing state responsibility for the cross-border attacks of non-state actors.

[289] *See* Proulx, *supra* note 283, at 660 (referencing this duty in regard to terrorism). State practice and *opinio juris* are the two elements that the international legal community recognizes as the basis for CIL. Jeremy Marsh, Lex Lata *or* Lex Ferenda*? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MIL. L. REV. 116, 121 (2008). State practices, state declarations, and United Nations General Assembly declarations and resolutions are all forms of state practice. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102 (1987) [hereinafter RESTATEMENT]. Furthermore, these declarations and resolutions serve as evidence of *opinio juris*. *Id.* § 103.

[290] *See* DINSTEIN, *supra* note 188, at 207.

[291] *See* Proulx, *supra* note 283, at 660 (discussing host-states' duty to stop acts of terrorism against other states when those attacks originate from within their borders).

[292] *See id.* at 662.

[293] *Id.*

C. Imputing State Responsibility for Acts by Non-State Actors

The question of a state's legal responsibility for the acts of non-state actors has evolved significantly during the past 37 years.[294] Before 1972, states were generally not viewed as legally responsible for the acts of private or non-state actors.[295] Only the conduct of the host-state's organs was imputable to it, and state responsibility arose only from acts by qualifying "agents" of the state.[296] Qualified agents amounted to actors whom a state exercised direct authority over, and whom the state directed to conduct the acts.[297] As time passed, international law shifted away from a direct control approach and moved toward an indirect responsibility approach regarding the acts of non-state actors.[298] This shift began with the International Tribunal for the former Yugoslavia's (ICTY) seminal opinion on state responsibility, in which it revised the effective control test to impute host-state responsibility for the actions of groups of non-state actors over whom a state had "overall control."[299]

[294] *See id.* at 616–19.

[295] *See id.* at 619.

[296] *See id.* at 619–20.

[297] *See* Proulx, *supra* note 283, at 620–21. The standard for assessing state responsibility under this paradigm was the "effective control test," which was first espoused by the ICJ in *Nicaragua*. In *Nicaragua*, the United States financed, organized, trained, supplied and equipped contra rebels, who were fighting against the government of Nicaragua. Yet despite the contras dependence on the United States, the ICJ refused to hold the United States legally liable for the contras' actions. The court took the view that while the United States provided decisive support to the contras, a state was not legally responsible for the actions of non-state actors unless the state "had effective control of the military or paramilitary operations in the course of which the alleged violations were committed." *Id.* at 620–21 (quoting the *Nicaragua* case). *But see* Mark Baker, *Terrorism and the Inherent Right of Self-Defense,* 10 HOUS. J. INT'L L. 25, 41 (1987) (raising the question that state responsibility might arise from the mere toleration of terrorist groups within a host-state's borders, without providing any active support).

[298] *See* Proulx, *supra* note 283, at 621–23.

[299] *See id.* (referring to the *Tadic* case, Prosecutor v. Tadic, Case No. IT-94-1-A, I.C.T.Y. App. Ch., at 49 (July 15, 1999), in which the court held that states were responsible for the acts of militarized groups when the state

While overall control is still a form of direct control, the opinion marked a significant relaxation of the standard for state responsibility.[300] The shift to indirect responsibility continued through the middle of 2001, with a general consensus emerging that any breach of a host-state's international obligations to other nations, whether from treaty law or customary law, resulted in international responsibility for the host-state.[301] These breaches can result from a state's acts or its failure to act.[302] This consensus solidified following the 9/11

coordinated or helped in the general planning of the group's military activity). This shift was not without precedence. In 1923, several members of an international commission, who were overseeing the delimitation of the Greek-Albanian border, were assassinated in Greek territory. The League of Nations organized a special committee to address the legal questions involved. While the committee found that the evidence did not support Greek responsibility, "it opined that a host-state could be held responsible in like circumstances if it 'neglected to take all reasonable measures for the prevention of the crime and pursuit, arrest and bringing to justice of the criminal.'" *Id.* at 627 (quoting the *Tellini* case, 4 League of Nations O.J. 524 (1924)).

While not yet culminating in a shift in international law, further precedence for the shift to indirect state responsibility comes from the *Tehran* case. In 1979, Iranian student militants took over the U.S. embassy and consulates in Iran. The ICJ found no evidence that the militants were operating on the direct behest of the Iranian state, and therefore found that the attacks could not be attributed to the state. However, the court also laid some blame on Iran, finding that "Iran was not 'free of any responsibility in regard to those attacks; for its own conduct was in conflict with its international obligations.'" "The court noted that Iran had a 'categorical duty' to protect the victims of the attack." It justified this position on the grounds that Iran bore indirect responsibility for its failure "'to take any appropriate steps . . . either to prevent this attack or to stop it before it reached its completion.'" *Id.* at 627–28 (quoting from the *Tehran* case, Tehran Hostages Case (U.S. v. Iran), 1980 I.C.J. 64 (May 24)).

Lastly, the trend toward indirect responsibility was evident in several cases before the Security Council in the 1990s. In several cases concerning international terrorism, the Security Council recognized the rights of injured states to pursue terrorists into other states to eliminate their bases of operation. Examples of such were in 1995–96 when Turkey pursued Kurdish irregulars on Iraqi soil; in 1992 and 1995 when Senegal entered Guinea-Bissau to strike at safe havens used by opposition forces; and in 1998 when the United States bombed parts of Afghanistan following terrorist attacks on U.S. embassies in Tanzania and Kenya. *See id.* at 630–31.

[300] *See id.* at 621.

[301] *See id.* at 622–23 (referencing the International Law Commission's adoption of the 2001 Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/Rev. 1 (2001)). After the International Law Commission approved the Draft Articles, the United Nations General Assembly took note of them and commended them to state governments on two different occasions; first in 2001 and next in 2004. *See* G.A. Res. 56/83, U.N. Doc. A/RES/56/83 (Jan. 28, 2002); G.A. Res. 59/35, U.N. Doc. A/RES/59/35 (Dec. 16, 2004).

[302] *See id.* at 626 (referencing Article 2 of the 2001 Draft Articles of the Responsibility of States for Internationally Wrongful Acts).

terrorist attacks on the United States, bringing us to today's framework for state responsibility.[303]

9/11 marked the culmination of the shift of state responsibility from the paradigm of direct control to indirect responsibility.[304] On September 11, 2001, Al Qaeda terrorists hijacked four airplanes and flew them into buildings in the United States, killing more than three thousand U.S. citizens, in what is widely recognized as an armed attack by non-state actors.[305] Al Qaeda was based in Afghanistan, which at the time was ruled by the Taliban.[306] While the Taliban harbored Al Qaeda and occasionally provided it limited logistical support, the Taliban did not exercise effective or even overall control over Al Qaeda.[307] Further distancing the Taliban from 9/11 is the lack of evidence suggesting that the Taliban knew of the 9/11 attacks beforehand, or even endorsed them after the fact.[308] Yet despite all of this, it was internationally accepted that Al Qaeda's acts were legally imputable to the Taliban, and thus Afghanistan, because it had harbored and sheltered Al Qaeda, and refused to stop doing so, even after being warned to stop.[309]

Thus, following 9/11, state responsibility basically results from a host-state's failure to fulfill its international duty to prevent non-state actors from using its territory to attack

[303] *See generally id.* at 618–19, 625–43 (explaining the shift from direct responsibility to indirect responsibility for the acts of non-state actors and the state of the law post-9/11).

[304] *See id.* at 634–52.

[305] Schmitt, *supra* note 264, at 33.

[306] *See* Proulx, *supra* note 283, at 634–37.

[307] *See id.* at 635–36.

[308] *See id.* at 636.

[309] *See id.* at 637–41.

other states.[310] The contemporary doctrine of state responsibility does not require a causal link between a wrongdoer and a host-state; rather, it focuses on the state's duty to prevent attacks from its territory into that of another.[311] "Hence, a state's passiveness or indifference toward [a non-state actor's] agendas within its own territory might trigger its responsibility, possibly on the same scale as though it had actively participated in planning."[312] Much of the legal analysis of whether a state is responsible will "turn on an ex-post facto analysis of whether the state could have put more effort into preventing the . . . attack."[313]

However, even when state responsibility is imputed for the armed attacks of non-state actors, states may still be limited from responding with force. The final step in the legal analysis for determining when victim-states can forcibly respond to the armed attacks of non-state actors ends with the legality of cross-border operations against other states.

D. Cross Border Operations

Cross-border operations into the territory of an offending state are the natural consequence of imputed state responsibility for the armed attacks of non-state actors.[314] However, states must meet a number of legal requirements before they may pursue a non-state aggressor into another state in self-defense, which are covered in this section. To

[310] *See* TAL BECKER, TERRORISM AND THE STATE: RETHINKING THE RULES OF STATE RESPONSIBILITY 3 (2006); 2001 Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/ Rev. 1 (2001).

[311] *See* BECKER, *supra* note 310, at 3; Proulx, *supra* note 283, at 633.

[312] Proulx, *supra* note 283, at 624.

[313] *Id.* at 663–64.

[314] *See* Schmitt, *supra* note 58, at 540–41.

understand the rationale behind why states may breach the host-state's general right to territorial integrity in self-defense and the requirements states must meet, one must first look to the U.N. Charter's general prohibition on using force against another state.

Article 2(4) of the U.N. Charter codified every state's general right of territorial integrity, a right also recognized by CIL.[315] Article 2(4) prohibits threats of force, uses of force and acts of aggression against the territorial integrity or political independence of another state, which is just another way of asserting that states enjoy a right to territorial integrity.[316] However, this right may be overridden in certain circumstances.[317]

The right of territorial integrity generally gives way to the right of self-defense.[318] The principle underlying this balancing act is that when one state violates another state's territorial integrity, it forfeits its own right to territorial integrity. This principle evolved out of state-on-state attacks. Nonetheless, this principle is applied in a similar manner when states are indirectly responsible for the violations of another state's territorial integrity by non-state actors.

> Ascertaining the appropriate balance between one State's right to territorial integrity and another's right to self-defense depends in part on the extent to which the former has complied with its own international obligations vis-à-vis the latter. It is a long-established principle of international law that "a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people."
> . . . .

[315] *See id.* at 540.

[316] *See id.*

[317] *See id.*

[318] After all, "it is manifestly legal to cross into another State to conduct military operations in self-defense if it is that State which has committed aggression." *Id.*

> If a State is unable or unwilling to comply with this obligation, the victim-state may then cross into the offending State to conduct defensive operations.
>
> . . . .
>
> It cannot be otherwise, for the unwillingness or inability of one State to meet its legal obligations cannot deprive other States of the most important right found in international law, the right to defend oneself against an armed attack.[319]

As always, before a state resorts to self-defense, it must ensure that it meets the criteria of necessity, proportionality, and, if utilizing the subset of anticipatory-self defense, imminency.[320] Effectively, a state must have no viable alternatives to the use of force, and it must limit its use of force to securing its defensive objectives.[321] Naturally, no two situations are alike, and justifications for self-defense are case-specific.

The application of these requirements may vary depending on whether the acts of the non-state actors were imputed based on direct control or indirect attribution. In cases of direct control, the victim-state may immediately fully impute responsibility to the host-state and act in self-defense against it and the non-state actors inside it.[322] In cases of indirect attribution, victim-states must overcome another hurdle before conducting cross-border operations. Namely, the victim-state must ensure that it has properly linked the actions of the non-state actors to the host-state; this may be achieved by issuing a demand to the sanctuary state to "comply with its obligation to prevent its territory from being improperly used."[323]

[319] *Id.* at 540–42 (quoting S.S. Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 4, 88 (Moore, J., dissenting)).

[320] *See id.* at 542.

[321] *See id.*

[322] *See id.* at 543.

[323] *Id.* at 542.

The sanctuary state must then act against the non-state actors, or willingly allow the victim-state to enter its territory and mount operations against the non-state actors.[324] Should the host-state be unwilling to meet these requirements, the victim-state can fully impute responsibility and conduct its cross-border operations into the host-state.[325] However, in doing so, the victim-state must limit its targets to the non-state actors, unless the host-state uses force to oppose the lawful cross-border operations.[326]

There are numerous examples of internationally accepted cross-border operations into states that were indirectly responsible for the actions of non-state actors. Examples prior to 9/11 include: Turkey's entrance into Iraq in 1995 to pursue Kurdish irregulars; Senegal's entrances into Guinea-Bissau in 1992 and 1995 to strike safe havens used by opposition forces; and the U.S. bombings of Afghanistan in 1998 to strike at terrorist training camps.[327] Post-9/11 examples include: Israel's initial entrance into Lebanon in 2006, following Hezbollah's raid into Israel;[328] and Turkey's air strikes into Iraq in 2007 against Kurdish irregulars.[329]

Based on the foregoing analysis, it is evident that victim-states may forcibly respond to armed attacks by non-state actors located in another state when the host-state violated its duty to prevent those attacks. With cyberattacks, imputing state responsibility in this manner

[324] *See id.* at 543.

[325] *See* Proulx, *supra* note 283, at 641–42; Schmitt, *supra* note 58, at 543; Mullerson, *supra* note 264, at 109.

[326] *See* Schmitt, *supra* note 58, at 543.

[327] *See* Proulx, *supra* note 283, at 630–31.

[328] *See* Greg Myre & Steven Erlanger, *Clashes Spread to Lebanon as Hezbollah Raids Israel*, N.Y. TIMES, July 13, 2006, at A1.

[329] *See* Sebnem Arsu & Stephen Farrell, *Turkey Bombs Kurds in Iraq; 2 Sides Differ on Casualties*, N.Y. TIMES, Dec. 23, 2007, at A27.

provides states a legal path to utilizing active defenses without having to conclusively attribute an attack to a state or its agents. In effect, imputing responsibility is the equivalent of attributing the attack to the state or its agents. Thus, imputing responsibility provides states a way around the attribution problem and response crisis. However, just because there is a legal pathway to get around the requirement that armed attacks be attributable to a state or its agents, does not mean that cyberattacks by non-state actors lend themselves to this framework. As a result, it is imperative to explain why cyberattacks constitute armed attacks, what a state's duty to prevent cyberattacks means, and the factual circumstances that would allow a victim-state to forcibly respond to a cyberattack, all of which are addressed in Part V.

V. Analyzing Cyberattacks under *Jus ad Bellum*

Cyberattacks represent a conundrum for legal scholars. Cyberattacks come in many different forms, their destructive potential only limited by the creativity and skill of the attackers behind them.[330] While it may seem intuitive that such attacks can constitute armed attacks, especially in light of their ability to injure or kill, the legal community has been reluctant to classify them this way because they do not resemble "classic attack[s] with traditional military force."[331] Further clouding the legal waters are the erroneous views of states and scholars alike on the need for states to attribute cyberattacks to a state or its agents

[330] WINGFIELD, *supra* note 49, at 100; *see also* Part II.A–B.

[331] THOMAS WINGFIELD, WHEN IS A CYBERATTACK AN "ARMED ATTACK?": LEGAL THRESHOLDS FOR DISTINGUISHING MILITARY ACTIVITIES IN CYBERSPACE 6 (Cyber Conflict Studies Assoc., 2006); *see also* GREENBERG ET AL., *supra* note 25, at xvii–xviii (noting the ambiguous state of international law regarding cyberattack classification).

before responding with force under the law of war. While it's true that cyberattacks don't resemble traditional armed attacks, and that cyberattacks are difficult to attribute, neither of these characteristics of cyberattacks should preclude states from responding with force under the law of war. This part explores different analytical models for assessing armed attacks, the logical meaning of the duty of prevention as it relates to cyberattacks, and the technological capacity of trace programs to trace attacks back to their point of origin. When all of these issues are tied together, it becomes obvious that states can legally take the crucial step of using active defenses to protect themselves from cyberattacks when a cyberattack originates from a state that violates its duty to prevent cyberattacks.

A. Cyberattacks as Armed Attacks

Being able to classify a cyberattack as an armed attack or imminent armed attack is an essential hurdle that victim-states must clear before responding with active defenses. This is because armed attacks and imminent armed attacks are the triggers that allow states to respond in self-defense or anticipatory self-defense.[332] Ideally, there would be clear rules for classifying cyberattacks as armed attacks, imminent armed attacks or lesser uses of force.[333] Unfortunately, since cyberattacks are a relatively new attack form, international efforts to classify them are still in their infancy,[334] even though the core legal principles governing

[332] *See supra* Part III.C–D.

[333] *See* WINGFIELD, *supra* note 331, at 1–2, 13. State coercion comes in three different forms: threats to international peace and security, uses of force, and armed attacks. *Id.* at 2. Threats to international peace and security and uses of force are both prohibited by Article 2(4) of the U.N. Charter. Armed attacks, including imminent armed attacks, are a more specific subset of uses of force that trigger a victim-state's inherent right of self-defense in response to them under Article 51 of the U.N. Charter. *See id.* at 4–5.

[334] *Id.* at 2–3, 13.

armed attacks are well settled.[335] This has left the questions of whether cyberattacks can qualify as armed attacks, and which cyberattacks should be considered armed attacks as open questions in international law.[336] To answer these questions, this section examines the core legal principles governing armed attacks, applies them to cyberattacks, explains why cyberattacks can qualify as armed attacks, and attempts to provide some insight as to which cyberattacks should be considered armed attacks.

"Armed attack" is not defined by any international convention.[337] As a result, its meaning has been left open to interpretation by states and scholars. While this might sound problematic, it is not. The framework for analyzing armed attacks is relatively well settled, as are the core legal principles governing its meaning.[338] The international community generally accepts Jean S. Pictet's scope, duration and intensity test as the starting point for evaluating whether a particular use of force constitutes an armed attack.[339] Under Pictet's

[335] *Id.* at 12.

[336] *Id.*

[337] *See* WINGFIELD, *supra* note 49, at 73 (noting the failure of international treaties to define "use of force," "armed force" or "armed attack").

[338] *See* WINGFIELD, *supra* note 331, at 12.

[339] *See* SHARP, SR., *supra* note 25, at 57–58 (referencing COMMENTARY ON THE GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 17–21 (Jean S. Pictet ed., 1958)); WINGFIELD, *supra* note 49, at 57, 60–68 (referencing COMMENTARY ON THE GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 17–21 (Jean S. Pictet ed., 1958)). Courts and scholars have also used a similar 'scale and effects' test to judge whether a particular attack rises to the level of an armed attack or constitutes a lesser use of force. *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 214–16 (June 27); DINSTEIN, *supra* note 188, at 193–96 (using the 'scale and effects' test from the *Nicaragua* case to assess armed attacks).

Pictet formulated this test to help clarify when international armed conflict exists under Common Article 2 of the Geneva Conventions. *See* SHARP, SR., *supra* note 25, at 57–58; WINGFIELD, *supra* note 49, at 57–60. Common Article 2 expresses three circumstances under which international armed conflict exists, and is widely accepted as the transition point between peace and war. WINGFIELD, *supra* note 49, at 57. The Common Article 2 circumstances are: a declared war between states, the partial or total occupation of another state, or any other armed conflict between states (also known as *de facto* hostilities). Geneva Convention for the Amelioration of test, a use of force is an armed attack when it is of sufficient scope, duration and intensity.[340] Of course, as is the case with many international legal concepts, states, non-governmental organizations and scholars all interpret the scope, duration and intensity test differently.[341]

State declarations help flesh out which uses of force are of sufficient scope, duration and intensity to constitute an armed attack. Harkening back to the French language version of the U.N. Charter, which refers to armed aggression rather than an armed attack, the U.N. General Assembly passed the Definition of Aggression resolution in 1974.[342] The resolution requires an attack to be of "sufficient gravity" before it's considered an armed attack.[343] While the resolution never defines armed attacks, it provides examples of them, which are

the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva I]. Once any of these circumstances are met, the threshold between peace and armed conflict is crossed, and the full body of the law of war applies in its entirety. *See* WINGFIELD, *supra* note 49, at 57–60. Since the first two situations are relatively straightforward, the bulk of the law focuses on what constitutes an armed conflict. *See id.*

The Geneva Conventions generally refers to the four Geneva Conventions of 1949. Article 2 of each convention is exactly the same, which is why it is called a common article. Individual citations are as follows: Geneva I, *supra* note 339; Geneva Convention for the Amelioration of the Condition of the Wounded, and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

[340] *See* WINGFIELD, *supra* note 49, at 57.

[341] *See* WINGFIELD, *supra* note 49, at 60–68, 111–23 (noting disagreements between the International Committee of the Red Cross's interpretation and the United States' interpretation, and reviewing different methods for evaluating the scope, duration and intensity cyberattacks); Brown, *supra* note 52, at 187–89 (discussing instrument-based evaluations of armed attacks versus effects-based evaluations of armed attacks).

[342] *See* WINGFIELD, *supra* note 49, at 111 (2000) (referencing Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974)).

[343] Definition of Aggression, G.A. Res. 3314, Annex, art. 2, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314/Annex (Dec. 14, 1974) (noting that the uses of force "shall constitute *prima facie* evidence of an act of aggression although the Security Council may . . . conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not of sufficient gravity").

widely accepted by the international community.[344] Unfortunately, the list of armed attacks from the resolution is not comprehensive as it only deals with conventional attacks.[345] While it has helped settle the meaning of armed attacks for conventional attacks, the more technology has advanced, the more attacks have come in forms not previously covered by state declarations and practices.[346] Consequently, states recognize that unconventional uses of force may warrant treatment as an armed attack when their scope, duration and intensity

[344] *See* WINGFIELD, *supra* note 49, at 111. Its view of what constitutes an armed attack encompasses:

> (a) *Invasion, bombardment and cross-border shooting*. These examples represent the classic cases of armed attacks, provided "that the military actions are on a certain scale and have a major effect, and are thus not to be considered mere frontier incidents."
>
> (b) *Blockade*. An effective blocking of a state's ports or coasts by the armed forces of another state is an armed attack. The barring of passage for land-locked states to the open sea across another state's territory has not been accepted as an armed attack.
>
> (c) *Attack on the land, sea or air forces or on the civilian marine and air fleets*. An armed attack occurs when the armed forces of one state attack the land, sea, or air forces, or the civilian marine and air fleets, of another state. The regular forces of a state, wherever they are, always have the right to defend themselves by military force.
>
> (d) *Breach of stationing agreements*. An armed attack may occur when a state uses its armed forces within the territory of another state in contravention of the conditions provided for in the agreement, or any extension of their presence beyond the termination of the agreement; provided, however, that the breach of the terms of the agreement has the effect of an invasion or occupation.
>
> (e) *Placing territory at another state's disposal*. The voluntary action of a state in allowing another state to use its territory for committing an armed attack is also an armed attack.
>
> (f) *Participating in the use of force by military organized unofficial groups*. It is widely accepted that indirect force falls under the definition of armed attack. The sending of armed bands to use force in another state makes the armed bands a *de facto* state agent, thus the sending state has engaged in an armed attack. Similarly, 'substantial involvement' in the activities of an armed band may also constitute an armed attack.

Id. at 111–12 (quoting THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 669–74 (Bruno Simma ed. 1994)).

[345] *See id.* at 112–15 (noting that the use of bacteriological, biological and chemical agents against another state is considered an armed attack, despite not being listed in the Definition of Aggression resolution).

[346] *See* WINGFIELD, *supra* note 49, at 113–15; QIAO LIANG & WANG WIANGSUI, UNRESTRICTED WARFARE 1–5 (1999) (speculating that technological advancement and globalization are changing warfare so that future wars will be carried out using non-military war operations, such as cyberattacks, in addition to conventional military force).

are of sufficient gravity.[347] As a result, states are continually making proclamations about new methods of warfare; slowly shaping the paradigm for classifying armed attacks.[348]

Scholars have advanced several analytical models to deal with unconventional attacks, such as cyberattacks, to help ease attack classification and put the scope, duration and intensity analysis into more concrete terms.[349] These models are especially relevant to cyberattacks because they straddle the line between criminal activity and armed warfare.[350] There are three main analytical models for dealing with unconventional attacks.[351] First is an instrument-based approach, which checks to see whether the damage caused by a new attack method could only have been previously achieved with a kinetic attack.[352] Second is an

[347] *See* WINGFIELD, *supra* note 49, at 100.

[348] For instance, the United States has made several declarations regarding cyberattacks, each of which generally infers that certain cyberattacks can be treated as armed attacks, provided their scope, duration and intensity have the same consequences as those normally associated with armed attacks. *See* Jensen, *supra* note 26, at 226–28; *see also* Department of Defense, Office of General Counsel, An Assessment of International Legal Issues, May 1999, *reprinted in* WINGFIELD, *supra* note 49, at 431 (treating cyberattacks as armed attacks when their consequences mirror those of an armed attack); Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996) (vowing to protect critical infrastructure against cyberattacks because their incapacitation or destruction could have a dehabilitating effect on U.S. defense and economic security); Exec. Order 13,321, 66 Fed. Reg. 53,063 (Oct. 16, 2001) (vowing to respond to cyberattacks against critical national infrastructure due to their potentially devastating effects on the United States).

[349] Brown, *supra* note 52, at 187–88.

[350] *See id.* at 187. Cyberattacks can be as simple as defacing a website, or as severe as crashing another state's stock markets and keeping them shut down for some time.

[351] *See* Brown, *supra* note 52, at 187 (discussing the instrument-based and effects-based approaches); Jensen, *supra* note 26, at 223–26 (discussing the strict liability and consequence-based approaches); Horace Robertson, Jr., *Self-Defense against Computer Network Attack*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 121, 134–38 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002) (discussing the consequence-based and strict liability approaches); Schmitt, *supra* note 56, at 913–17 (discussing the instrumented-based and consequence-based approaches).

[352] *See* Brown, *supra* note 52, at 187–88; Dinstein, *supra* note 25, at 103–05. For instance, under an instrument-based approach, a cyberattack used to shut down a power grid is an armed attack. This is because shutting down a power grid typically required dropping a bomb on a power station or some other kinetic use of force to incapacitate the grid. Since conventional munitions were previously required to achieve the result, under the instrument-based approach the cyberattack is therefore treated the same way.

effects-based approach, sometimes called a consequence-based approach, in which the attack's similarity to a kinetic attack is irrelevant and the focus shifts to the overall effect that the cyberattack has on a victim-state.[353] This happens to be the approach that the United States has adopted.[354] Third is a strict liability approach, in which cyberattacks against CNI are automatically treated as armed attacks, due to the severe consequences that can result from disabling those systems.[355] While these analytical models differ, the common thread between them is that the proponents of each analytical model all agree that cyberattacks can constitute an armed attack.[356] In fact, a large number of the scenarios covered in Part II, Section B fit into the meaning of armed attack under all three models of analysis.[357] Cyberattacks short of armed attacks would still be considered an unlawful use of force in

[353] *See* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 362–63 (1963); WINGFIELD, *supra* note 49, at 117–30; Brown, *supra* note 52, at 187–88; Schmitt, *supra* note 3, at 1071–72; Schmitt, *supra* note 56, at 911–15. For instance, under an effects-based approach, a cyberattack that manipulated information across a state's banking and financial institutions to seriously disrupt commerce in the state is an armed attack. While the manipulation of information does not resemble a kinetic attack, as required under an instrument-based approach, the disruptive effects that the attack had on the state's economy is a severe enough overall consequence that it warrants treatment as an armed attack.

[354] *See* Department of Defense, Office of General Counsel, An Assessment of International Legal Issues, May 1999, *reprinted in* WINGFIELD, *supra* note 49, at 431, 453–54.

[355] It is important to note that this third analytical model for dealing with cyberattacks is intended to justify anticipatory self-defense before any harm actually results. Walter Gary Sharp, Sr. proposed this model due to the speed with which a computer penetration can transition into a destructive attack against defense CNI. His reasoning is that once a penetration has occurred, an imminent threat exists with the ability to cause harm of extreme scope, duration and intensity, thereby justifying anticipatory self-defense. *See* SHARP, SR., *supra* note 25, at 129–31; *see also* Condron, *supra* note 25, at 415–22 (discussing the need to treat cyberattacks on CNI as armed attacks); Jensen, *supra* note 26, at 228–31(advocating changing the current *jus ad bellum* paradigm to use strict liability for cyberattacks against CNI).

[356] *See* WINGFIELD, *supra* note 49, at 117–30; Brown, *supra* note 52, at 190; Dinstein, *supra* note 25, at 103–05; Schmitt, *supra* note 56, at 911–15; Robertson, Jr., *supra* note 351, at 134–38; Condron, *supra* note 25, at 415–22; Jensen, *supra* note 26, at 228–31; KAMAL, *supra* note 23, at 76–84.

[357] *See* WINGFIELD, *supra* note 49, at 117–30; Brown, *supra* note 52, at 187–88; Dinstein, *supra* note 25, at 103–05; Schmitt, *supra* note 56, at 911–15; Robertson, Jr., *supra* note 351, at 134–38; Condron, *supra* note 25, at 415–22; Jensen, *supra* note 26, at 228–31; KAMAL, *supra* note 23, at 76–84.

violation of Article 2(4) of the U.N. Charter,[358] and would have to be met with measures short of self-defense, such as a reprisal.[359]

Of these three approaches, the effects-based approach is the best analytical model for dealing with cyberattacks. Not only does effects-based analysis account for everything that instrument-based approaches cover, but it also provides an analytical framework for situations that do not neatly equate to kinetic attacks.[360] Effects-based analysis is also superior to strict liability because responses to cyberattacks under an effects-based approach comport with internationally accepted legal norms and customs, whereas a strict liability approach can easily lead victim-states to commit law of war violations.[361]

[358] *See* WINGFIELD, *supra* note 49, at 91–99 (discussing cyberattacks that don't rise to the level of an armed attack). Unfortunately, trying to formulate an exact line to delineate armed cyberattacks from lesser uses of force is nearly impossible. Thus, this section shall advance several analytical models to help classify attacks, recognizing that it will be up to victim-states to form the view and declare whether particular cyberattacks against them are armed attacks, and to be ready to defend their conclusion to the international community.

[359] This is because at a minimum, cyberattacks are an illegal use of force. As a result, states can use reprisals to deter attackers from attacking in the future, and deter sanctuary states from allowing attackers to commit them. *See supra* Part III.E (discussing reprisals); *supra* Part IV.E (discussing sanctuary states that allow attackers to act inside their borders); *infra* Parts V.C (discussing state responsibility for failing to prevent cyberattacks).

[360] For instance, a cyberattack might shut down a system, rending it inoperable for some time, or a cyberattack might cause an explosion at a chemical plant by tampering with the computers that controlled the feed mixture rates. The results of those attacks mirror the results of conventional armed attacks, previously only achievable through kinetic force, thus satisfying the instrument-based approach.

Unfortunately, cyberattacks can cause extreme harm without mirroring the results of conventional armed attacks. For instance, coordinated cyberattacks could bring financial markets to their knees without ever employing anything that looked remotely like a kinetic attack; altered data on a massive scale could disrupt banking, financial transactions and the general underpinnings of the economy, sowing confusion throughout the victim-state for some time. Under an effects-based approach, the scope, duration and intensity of this attack would equate to an armed attack, despite the fact that it wasn't previously only achievable through kinetic force.

[361] The proponents of a strict liability approach advocate automatically responding to cyberattacks on critical infrastructure with active defenses. *See* Condron, *supra* note 25, at 415–22; Jensen, *supra* note 26, at 228–31. However, automatically responding to cyberattacks in this manner can easily lead a victim-state to counter-attack a state with a long history of doing everything within its power to prevent cyberattacks and prosecute its attackers. Were a victim-state to respond with active defenses against a non-sanctuary state, it would violate *jus ad bellum*. This is because there is no way to impute state responsibility to such a state, directly or indirectly, even though the cyberattack may constitute an armed attack. *See supra* Part IV.C.

Of all of the scholars who advocate effects-based models, Michael N. Schmitt has advanced the most useful analytical framework for evaluating cyberattacks. In his seminal article, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, Michael Schmitt lays out six criteria for evaluating cyberattacks as armed attacks.[362] These criteria are severity,[363] immediacy,[364] directness,[365] invasiveness,[366] measurability,[367] and presumptive legitimacy.[368] Taken together, these criteria allow states to measure cyberattacks along several different axes. While no one criterion is dispositive, cyberattacks that possess enough of the qualities of an armed attack, should indeed be characterized as such.[369] Since their publication, Schmitt's criteria have gained traction in

[362] Schmitt, *supra* note 56, at 913–15.

[363] Severity looks at the scope and intensity of an attack. Analysis under this criterion would include looking at the number of people killed, size of the area attacked, and amount of property damage done. The greater the damage, the more powerful the argument becomes for treating the cyberattack as an armed attack. *See* WINGFIELD, *supra* note 49, at 124–27 (examining Michael Schmitt's use of force analysis).

[364] Immediacy looks at the duration of a cyberattack, as well as other timing factors. Analysis under this criterion looks at how long the cyberattack lasted, how soon its effects were felt, and how long it took for the effects to abate. The longer the duration and effects, the more it looks like an armed attack. *See id.* (examining Michael Schmitt's use of force analysis).

[365] Directness looks at the harm caused. If the attack was the proximate cause of the harm, it strengthens the argument that the cyberattack was an armed attack. If the harm was caused in full or in part by other parallel attacks, the weaker the argument that the cyberattack was an armed attack. *See id.* (examining Michael Schmitt's use of force analysis).

[366] Invasiveness looks at the locus of the attack. An invasive attack is one that physically crosses state borders, or electronically crosses borders and causes harm within the victim-state. The more invasive the cyberattack, the more it looks like an armed attack. *See id.* (examining Michael Schmitt's use of force analysis).

[367] Measurability tries to quantify the damage done by the cyberattack. Quantifiable harm is generally treated more seriously in the international community. The more a state can quantify the harm done to them, the more the cyberattack looks like an armed attack. Speculative harm generally makes a weak case that the cyberattack was an armed attack. *See id.* (examining Michael Schmitt's use of force analysis).

[368] Presumptive legitimacy focuses on state practice and the accepted norms of behavior in the international community. Actions may gain legitimacy under the law when the international community accepts certain behavior as legitimate. The less a cyberattack looks like accepted state practice, the stronger the argument that it is an illegal use of force or an armed attack. *See id.* (examining Michael Schmitt's use of force analysis).

[369] *See id.* at 122–29 (examining Michael Schmitt's use of force analysis).

the legal community, with several prominent legal scholars advocating for their use.[370] Hopefully Schmitt's criteria will help bring some uniformity to state efforts to classify cyberattacks by providing common criteria to evaluate cyberattacks. However, until Schmitt's criteria gain wider acceptance, states are likely to classify cyberattacks differently, depending on their approach to armed attacks, as well as their conception of vital national interest.[371] Moreover, universal acceptance of Schmitt's criteria is still probably some time off, as effects-based analysis is not free from criticism.

Detractors generally critique effects-based analysis as useful only long after a cyberattack occurs; arguing that cyberattacks force states to make rapid decisions with little information, and that performing an effects-based analysis forces states to delay their responses to the point that the state suffers preventable harm.[372] More specifically, some detractors acknowledge that effects-based analysis may be useful, but advocate treating all cyberattacks on CNI as armed attacks on the grounds that it is too dangerous to waste time analyzing the attack when CNI is at risk.[373] These detractors generally advocate a strict liability approach to cyberattacks against CNI, and further advocate responding to all cyberattacks against CNI in self-defense as the only effective method to protect CNI.[374]

[370] *See* WINGFIELD, *supra* note 331, at 6–7; WINGFIELD, *supra* note 49, at 115–29 (2000); Vida Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?*, 51 NAVAL L. REV. 132, 169–72 (2005); Robertson, Jr., *supra* note 351, at 134–38.

[371] *See* WINGFIELD, *supra* note 331, at 8.

[372] *See* Barkham, *supra* note 30, at 83–84.

[373] *See* Condron, *supra* note 25, at 415–22 (advocating strict liability for cyberattacks on CNI); Jensen, *supra* note 26, at 228–31 (advocating strict liability for cyberattacks on CNI).

[374] *See* Condron, *supra* note 25, at 415–22; Jensen, *supra* note 26, at 228–31.

While the proponents of strict liability have correctly identified a grave threat to state security, their model sells effects-based analysis short and runs the risk of unlawfully escalating a situation. In no way does effects-based analysis require a state to delay its response until it can fully measure a cyberattack against all six of Schmitt's proposed axes. Decision-makers, at times, must make choices with imperfect information. "As a legal matter, however, the principle of anticipatory-self-defense does not, and has never, required that the threat have been genuine—only that it be perceived to be so in good faith."[375] The imminent danger that some cyberattacks pose will force decision-makers to attempt a good faith assessment based on the facts at hand. Other cyberattacks will not be as urgent, allowing decision-makers to take time to analyze the attacks more fully. In all cases, an effects-based approach provides a better analytical tool by which to analyze an attack. Furthermore, when a threat is considered urgent, such as an attack against CNI, the potential severity and imminence of the attack may be great enough to outweigh all other considerations. Furthermore, even if cyberattacks against CNI generally constitute armed attacks, automatically responding to them in self-defense may result in the use of force against an innocent state, i.e., one that does not meet the threshold for imputing state responsibility.[376]

[375] David Rivkin, Jr. et al., *War, International Law, and Sovereignty: Reevaluating the Rules of the Game in a New Century: Preemption and Law in the Twenty-First Century*, 5 CHI. J. INT'L L. 467, 496 (2005); *see also* Eric Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1181–82 (2003) (discussing United States v. Wilhelm List, XI Trials of War Criminals Before the Nuremburg Military Tribunals Under Control Council Law No. 10, 1295–96 (1950)). The legal standard for judging a military commander's decision is whether what the commander believed to be true at the time (not the actual facts) met the appropriate legal standards. This is known as the Rendulic Rule, and has been the international standard since the Nuremburg trial of General Rendulic. *Id.*

[376] State responsibility for cyberattacks may be established when states violate their duty to prevent cyberattacks. *See infra* Part V.B–C.

Classifying cyberattacks will be difficult for states to do in actual practice.[377] While the decision to respond to cyberattacks under the law of war will have to be made by state decision-makers, the actual decision to use active defenses will have to be pushed down to the system administrators who actually operate computer networks. One of the challenges states will face is translating international law into concise, understandable rules for their system administrators to follow, so that a state's agents comply with international law while protecting its vital computer networks. However, classifying cyberattacks as armed attacks or imminent armed attacks is only the first hurdle system administrators must clear before responding with active defenses. The second and equally important hurdle is establishing state responsibility for the attack.

[377] While classifying cyberattacks will be difficult, there is no doubt that some cyberattacks will qualify as armed attacks, and should be dealt with using self-defense and anticipatory self-defense legal principles as a justification for using active defenses.

Some scholars will undoubtedly critique this paper's conclusion that cyberattacks can qualify as armed attacks. However, scholars who argue that cyberattacks cannot rise to the level of armed attacks miss the way the law has responded to unconventional attacks in the past. New attack methods frequently fall outside the accepted definitions of armed attacks. This does not mean that the attacks are not armed attacks, merely that the attacks don't fit traditional classifications. There are several analytical models for classifying new attack forms, all of which are based on the accepted core legal principles that were used to classify conventional attacks. Of these, the effects-based approach proposed by Michael N. Schmitt has the greatest analytical power and makes the most sense to use. *See supra* Part V.A (discussing the attack classification of new attack forms). Furthermore, scholars who advocate that cyberattacks cannot rise to the level of armed attacks miss an important facet of international law—reprisals, which can be used as an alternate basis to authorize active defenses against cyberattacks should the international community reject this paper's conclusion and classify cyberattacks as lesser uses of force. This is because at a minimum, cyberattacks are an illegal use of force. As a result, states can use reprisals to deter attackers from committing such acts in the future, and to deter sanctuary states from allowing attackers to commit them. *See supra* Part III.E (discussing reprisals); *infra* Part V.B–C (discussing state responsibility for failing to prevent cyberattacks).

As an important sidebar, reprisals may theoretically justify using active defenses to protect non-vital computer systems. Since attacks on non-vital computer systems amount to an illegal uses of force, reprisals may provide a justification for defending those systems with active defenses (assuming the active defenses targeted non-vital systems in return). In effect, active defenses may provide a way to deter cyberattacks in general. On these grounds, private corporations or individuals could theoretically attempt to justify defending their systems with active defenses based on the general principles of self-defense recognized by most nations. However, as this would most likely result in non-state actors using active defenses across state borders, it would raise a host of other questions under international law. The ideas covered in this sidebar are beyond the scope of this paper, but are worthy of consideration.

B. Modernizing the Approach to State Responsibility for Cyberattacks

States cannot respond to a cross-border cyberattack with force without establishing state responsibility for the attack.[378] Traditionally, this meant attributing an attack to a state or its agents on the premise that a state is only responsible for its acts or the acts of those under its direct control.[379] However, as non-state actors have attacked states with increased frequency, international law has shifted away from this traditional requirement to a model of indirect state responsibility based on a state's failure to meet its international duties.[380]

This shift is especially important for cyberattacks because the prevailing view that states must treat cross-border cyberattacks as a criminal matter, rather than as a national security matter, seems to be based on the traditional view of state responsibility, which ignores the shift in the law of war toward indirect state responsibility. This limited view of state responsibility locks states into the response crisis by requiring states to attribute cyberattacks to a state or its agents,[381] even though the likelihood of successfully achieving such attribution is extremely remote.[382] Consequently, states that subscribe to the traditional

[378] *See supra* Part IV.D.

[379] *See supra* Part IV.C.

[380] *See id.*

[381] *See supra* Part II.B; *supra* Part IV, introduction.

[382] A cyberattack could be directly linked to a state under a few circumstances. Potential direct links might include a state declaration that it had made the attack; pre-attack intelligence suggesting that a state was about to make an attack; or tracing an ongoing attack to computer systems known to belong to a foreign military.

Further complicating the attribution problem is that cyberterrorists and cybercriminals often hijack innocent systems and use them as zombies to initiate their cyberattacks. *See supra* Part II.A. While victim-states must try to penetrate such guises, current technology may not always allow them to do so in a timely manner. *See* Brown, *supra* note 52, at 201. In effect, attackers complicate the decision-making process of victim-states, who must account for these electronic disguises when trying to attribute the true identity of an attacker.

model of state responsibility will find themselves in the response crisis during a cyberattack, laboring under the false assumption that they must decide between effective, but illegal, active defenses, and the less effective, but legal, path of passive defenses and host-state criminal laws.[383]

Given the shift in the law of state responsibility, states should determine whether a cyberattack can be imputed to the state of origin, rather than trying to conclusively attribute it. This is because once a cyberattack is imputed to a state, the legal barriers to acting in self-defense disappear.[384] States that continue to follow the prevailing view of state responsibility will unduly limit their right to use active defenses, and increase the chances of a successful cyberattack against them.[385] Considering the catastrophic consequences that a cyberattack can have, states should not follow the prevailing view when the law does not require them to do so.

While neither state practice nor the publications of legal scholars support this view regarding cyberattacks yet,[386] the accepted principles of customary *jus ad bellum* support

[383] *See supra* Part II.B; *supra* Part IV, introduction.

[384] *See supra* Part IV.C–D.

[385] *See* Condron, *supra* note 25, at 415–22; Jensen, *supra* note 26, at 228–31.

[386] Legal scholars generally agree that states may not respond in self-defense until after an attack is attributed. *See* Condron, *supra* note 25, at 415; Dinstein, *supra* note 25, at 111; Garnett & Clarke, *supra* note 13, at 478–79. As a result, state practice is currently to respond to cyberattacks with passive defenses and host-state criminal laws. *See* Condron, *supra* note 25, at 407; Hollis, *supra* note 23, at 1050. States may also seek to extradite an attacker and deal with them under their own laws; however, absent an extradition treaty with the host-state, states have no legal right to demand extradition of foreign nationals. *See* Factor v. Laubenheimer, 290 U.S. 276, 287 (1933); KAMAL, *supra* note 23, at 215–22.

However, there is a growing recognition among legal scholars that the current paradigm governing state responses to cyberattacks is inadequate to protect states and it must change. *See supra* note 52. The scholars who argue against the current paradigm have tried to solve the response crisis by finding creative ways around the attribution problem. The three main proposals advanced by scholars before this paper are discussed below.

One group of scholars advocates a strict liability approach to attacks against CNI. Eric Jensen first argued for this approach, on the basis that attacks against CNI automatically demonstrates hostile intent. Jensen's proposal argues that states should publish a list of systems that they deem to be CNI, which they would respond to in anticipatory self-defense in the case of a cyberattack. He argues that publishing a list of CNI puts attackers on notice, which can then be used as a tool to determine the intent of an attacker. "It should be made clear that once an intruder has shown the intent and capability to pierce the passive defense measures of [CNI], he has demonstrated sufficient hostile intent to warrant an action in self-defense, even though he may not yet have consummated his attack." *See* Jensen, *supra* note 26, at 236–37. Sean Condron supports this approach, arguing that international law should grant states an exception to use active defenses to protect CNI, due to the grave harm that cyberattacks against them can cause. *See* Condron, *supra* note 25, at 415–22.

Another group of legal scholars advocate that self-defense is always a legal response to armed attacks. Their rationale is that the U.N. Charter does not subsume a state's inherent right of self-defense under CIL, which includes a right to respond to armed attacks by non-state actors. Thus, states can always respond to cyberattacks that amount to an armed attack because the attack was either conducted by a state, which allows them to respond under Article 51 of the U.N. Charter, or was conducted by a non-state actor, which allows them to respond under CIL. *See* Barkham, *supra* note 30, at 104; Schmitt, *supra* note 56, at 933–34.

Finally, two legal scholars correctly hone in on state responsibility as the solution to the attribution problem. However, instead of tying state responsibility to their failure to meet their duty to prevent cyberattacks, they contend that when cyberattacks are repeatedly launched from one state against other states, the state of origin should be presumed to have knowledge of and involvement in the attacks. Following this logic, these scholars argue that victim-states can hold host-states responsible for cyberattacks based on their assumed control of the non-state actors. Garnett & Clarke, *supra* note 13, at 479.

While the three approaches suggested above have less of a basis in international law than the approach suggested by this paper, these scholars' ideas on getting around the attribution problem are not without merit. Right now, states are stuck in the uncomfortable position of relying on passive defenses and host-state criminal laws. Naturally, states will want to defend their systems with active defenses, especially their critical systems. While something more needs to be done, automatically responding to cyberattacks against critical systems with active defenses may inadvertently counter-attack states that meet their duty to prevent cyberattacks. *See supra* Part I.B (discussing the response crisis); *supra* Part IV, introduction (discussing the response crisis).

During a cyberattack, system administrators can frequently trace the electronic pathways that cyberattacks follow back to their source. *See generally* Wheeler & Larsen, *supra* note 162 (for a technical discussion on tracing cyberattacks back to their point of origin). When an attack is traced to a state that turns a blind eye to cyberattacks, such as China or Russia, responding with active defenses seems like a wise and legal option. This is because these states have demonstrated an unwillingness to prevent cyberattacks or cooperate with victim-states. However, when an attack is traced back to a state that takes affirmative steps to deter cyberattacks and always works its hardest to investigate and prosecute attackers, such as the United Kingdom, automatically responding with force does not seem wise or legal, as the host-state is following its international duty.

Scholars who advocate responding to armed cyberattacks regardless of an attacker's identity would, no doubt, critique this paper's approach as not going far enough to protect CNI, since it only protects CNI against attacks originating from sanctuary states; thus, leaving CNI vulnerable to attacks that originate elsewhere. As discussed earlier, these scholars raise a valid concern about the safety of state CNI. However, their argument misses a critical part of the legal analysis. Namely, just because a state's CNI is under attack by non-state actors does not give the victim-state legal authority to violate the territorial integrity of a host-state and respond with force. Such a right only arises when state responsibility has been established. Were a state to follow the path advocated by these scholars, the fears of the scholars who don't believe in active defenses would be realized. Automating active defenses will result in counter-attacks against every attacking computer across the world, regardless of their state of origin. While targeting the systems of states that choose not to take part in the international community's efforts to eradicate cyberattacks is an acceptable and lawful option, it is unacceptable and unlawful to target states that fully participate in international efforts to secure cyberspace.

indirectly imputing state responsibility for armed attacks by non-state actors when the attacks originate from a state that allows non-state actors to conduct criminal operations within their borders.[387] States that allow non-state actors to conduct those operations breach their duty to prevent attacks against other states, and are known as sanctuary states.[388] This is extremely important to the victim-states of cyberattacks because when a cyberattack originates from a sanctuary state, a victim-state may employ active defenses and avert the response crisis.

It is thus necessary to understand the answers to two key questions: (1) What is a state's duty to prevent cyberattacks? and (2) What must a state do to violate its duty of prevention? The answers to these questions are the legal keys that will establish the basis for imputing state responsibility for cyberattacks, and unlock the restraints that states have placed on themselves by unnecessarily following the prevailing view of state responsibility.

C. The Duty to Prevent Cyberattacks

States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, which together constitute a state's duty of prevention. These duties include: passing stringent criminal laws against international cyberattacks, conducting vigorous investigations into international cyberattacks, prosecuting attackers who have conducted international cyberattacks, and cooperating with the victim-states of cyberattacks that originated from within their borders during the

[387] *See supra* Part IV.C (reviewing the principles of state responsibility).

[388] *See supra* Part IV.B (reviewing the duty to prevent non-state actors from using a state's territory to commit criminal acts against another state); *supra* Part IV.D (reviewing sanctuary states and the legality of holding them responsible for the actions of those non-state actors).

investigation and prosecution. These duties are the duties of all states, and, as will be shown in this section, are binding as CIL.[389] The authority for these duties comes from all three sources of CIL—international conventions, international custom, and the general principles of law common to civilized nations, as also evidenced by judicial decisions and the teachings of the most highly qualified international legal scholars.

1. Support from International Conventions

The only international treaty directly on point is the European Convention on Cybercrime. While the treaty is only a regional agreement, it is still very influential on CIL because of the importance of the states that have ratified it under the specially affected states doctrine.[390] Furthermore, it demonstrates state recognition of both the need to criminalize

[389] Customary international law is one of the principal sources of international law. RESTATEMENT, *supra* note 289, § 102.   When a legal principle becomes recognized as customary international law, it becomes a binding legal obligation on all states. *Id.* Customary international law is formed through state practice and *opinio juris sive necessitates* (a sense of legal obligation on the part of states to engage in a practice). *Id.* International agreements, state practice, state declarations and United Nations General Assembly resolutions all count as forms of state practice. *Id.* § 102–03. Furthermore, judicial opinions and the writings of international scholars may both be used as evidence of state practice and *opinio juris*. *Id.* § 103.

The other principal source of international law is international agreements. *Id.* § 102. The third and somewhat ancillary source of international law is the general principles of law common to the major legal systems of the world; however, this is infrequently used as a source of international law. An example of a general legal principle is the prohibition on torture in most domestic legal systems.   *Id.*

These definitions roughly mirror the sources of international law found in the Statute of the ICJ. The Statute of the ICJ lists four sources of international law, the first three of which mirror these sources of international law, and then uses judicial opinions and the publications of scholars as a subsidiary means for determining the law. Furthermore, the statute's description of international custom roughly mirrors the Restatement's description of CIL. *See* Statute of the International Court of Justice, art. 38(1), June 26, 1945, 59. Stat. 1055, 1060 (1945).

[390] Customary international law does not require state practice to be universal. General practices can satisfy the requirements of customary international law. The test for when state practices become customary international law is when the practice is extensive and representative. "That is to say, it is not simply a question of how many States participate in the practice, but also *which* States." Jean-Marie Henckaerts, *Customary International Humanitarian Law Study: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, *in* THE LAW OF WAR IN THE 21ST CENTURY: WEAPONRY AND THE USE OF FORCE 37, 42

cyberattacks, and the duty of states to prevent their territory from being used by non-state actors to conduct cyberattacks against other states.[391] The Convention is also significant because it recognizes that cyberattacks cannot be interdicted during the middle of an attack, and that the only way to prevent them is through aggressive law enforcement, coupled with state cooperation.[392]

International treaties to criminalize terrorism provide further support, albeit indirectly, for the duty to prevent cyberattacks. The international community recognizes

(Anthony M. Helm ed., Naval War College 2006). This is where the specially affected state doctrine comes into play. When states whose interests are specially affected by a practice all follow the practice, the practice becomes CIL even if the majority of states do not participate, as long as the majority acquiesces to the practice. Likewise, even if the majority of states declare something to be CIL, if the specially affected states do not accept the practice, it cannot become CIL. *Id.* at 42–43. In other words, states whose interests are especially affected by a particular state practice are specially affected states, and their practices carry more weight in contributing to CIL about that practice. Yoram Dinstein, *The ICRC Customary International Law Study*, *in* THE LAW OF WAR IN THE 21ST CENTURY: WEAPONRY AND THE USE OF FORCE 99, 109 (Anthony M. Helm ed., Naval War College 2006). The specially affected states doctrine was developed by the ICJ in the *North Sea Continental Shelf* cases. North Sea Continental Shelf (F.R.G. v. Den.; F.R.G. v. Neth.), 1969 I.C.J 3, 43 (Feb. 20).

To date, twenty-two states have ratified the Convention on Cybercrime, the majority of which are major western powers, six of which place among the twelve states with the most internet users in the world—France, Germany, Italy, the Netherlands, the United Kingdom and the United States. Together, these six states have more internet users than all of the remaining states that make up the top twenty states with the most internet users in the world. Furthermore, three of these states are permanent members of the U.N. Security Council—France, the United Kingdom and the United States. The United States is the only non-European state to ratify the treaty. Furthermore, while not yet parties to the treaty, Canada, Japan, Spain, Poland and Sweden are all signatories to it, and are expected to ratify it soon. These five states are all among the remaining twenty states with the most internet users in the world, and their ratification of the treaty would greatly move state practice to the standards set forth in the convention. *See* Council of Europe, Convention on Cybercrime, Chart of Signatures and Ratifications, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=18/06/04&CL=ENG (listing the twenty-four signatories and twenty-two parties to the Convention on Cybercrime) (last visited Mar. 19, 2009); COLARIK, *supra* note 6, at 151 (listing the top twenty states with the most internet subscribers in 2005).

[391] The Convention on Cybercrime requires the parties to it to establish criminal offenses for almost every conceivable type of cyberattack under their domestic laws. *See* Convention on Cybercrime, *supra* note 23, art. 2–11, at 284–87. It also recognizes the importance of prosecuting attackers, which is demonstrated by its requirement for states to extend their jurisdiction over any cyberattacks conducted from within their territory, or conducted by their citizens regardless of their location at the time of attack. *See id.*, art. 22, at 291–92. Finally, the convention recognizes the importance of state cooperation to hunt down attackers and bring them to justice; requiring states to cooperate with each other and provide "mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences." *See id.*, art. 23–25, at 292–93.

[392] *See* KAMAL, *supra* note 23, at 71.

terrorism as a threat to international peace and security, but cannot agree on a definition for it.[393] As a result, states have adopted the approach of outlawing specific terrorist acts each time terrorists adopt new attack methods, rather than outlawing terrorism itself.[394] These treaties impose several common requirements on states with regard to terrorist attack methods, such as: taking all practicable measures for the purpose of preventing these attacks, criminalizing the attacks, submitting cases to competent authorities for prosecution, and forcing states to cooperate with each other throughout the criminal proceedings.[395] While these treaties do not address cyberattacks, the principles contained in them help influence state requirements under CIL with regard to terrorism. Since there is growing evidence that

[393] Pierre-Marie Dupuy, *State Sponsors of Terrorism: International Responsibility*, *in* ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 3, 4–6 (Andrea Bianchi ed., 2004). "One of the reasons why it has been difficult to secure a universally accepted definition of terrorism has been that some States, primarily from the developing world, have sought to resist condemnation of practices and activities which they may have resorted to in their acquiring of independence, particularly during decolonization." Gannett & Clarke, *supra* note 13, at 466.

[394] Dupuy, *supra* note 393, at 4–6; Gannett & Clarke, *supra* note 13, at 466. These treaties include the 1963 Tokyo Convention on Offences and Certain Other Acts Committed on Board Aircraft, 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft, the 1971 Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, 1979 International Convention Against the Taking of Hostage, 1988 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988 Montreal Protocol on the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, 1997 International Convention for the Suppression of Terrorist Bombings, 1999 International Convention for the Suppression of the Financing of Terrorism, and 2005 International Convention for the Suppression of Acts of Nuclear Terrorism. *See* Dupuy, *supra* note 393, at 4–6 (using several of these treaties as examples of treaties that outlawed particular terrorist attack methods); Gannett & Clarke, *supra* note 13, at 466 (using several of these treaties as examples of treaties that outlawed particular terrorist attack methods).

[395] *See generally* Hague Convention for the Suppression of Unlawful Seizure of Aircraft, *done* Dec. 16, 1970, 22 U.S.T. 1641, T.I.A.S. No. 7192; Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation, *done* Sept. 23, 1971, 24 U.S.T. 564, T.I.A.S. No. 7570; International Convention Against the Taking of Hostage, *opened for signature* Dec. 18, 1979, 18 I.L.M. 1456; Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, *done* Mar. 10, 1988, 1678 U.N.T.S. 221, 27 I.L.M. 668; International Convention for the Suppression of Terrorist Bombings, *opened for signature* Jan. 12, 1998, 37 I.L.M. 249; International Convention for the Suppression of the Financing of Terrorism, *opened for signature* Jan. 10, 2000, 39 I.L.M. 270; International Convention for the Suppression of Acts of Nuclear Terrorism, *opened for signature* Sept. 14, 2005, 44 I.L.M. 815.

cyberattacks will soon be a weapon of choice for terrorists,[396] states should follow the common principles found in these treaties as *opinio juris* when cyberattacks are used as a terrorist weapon.

2. *Support from State Practice*

State treatment of cyberattacks under their criminal laws also evidence recognition of the duty to prevent cyberattacks under CIL. Numerous states criminalize and prosecute cyberattacks as a way to deter attackers from conducting them, on the basis that vigorous law enforcement is the only way to protect and prevent harm to their computer systems.[397] This lends credence to the notion that, unlike a conventional attack which can be stopped after detection, cyberattacks can only be stopped by establishing *ex ante* barriers that attackers are fearful of crossing. Furthermore, these state practices demonstrate a growing recognition among states that cyberattacks must be stopped, and that the way to do so is through vigorous state law enforcement.

[396] Garnett & Clarke, *supra* note 13, at 467; ROLLINS & WILSON, *supra* note 15, at CRS-1.

[397] *See* KAMAL, *supra* note 23, at 176. Australia's Cyber-Crime Act of 2001 criminalizes the unauthorized access or modification of computer data. Austria's Privacy Act of 2000 criminalizes the unauthorized access of any computer data. Belgium's criminal code targets computer crime and basically outlaws all forms of cyberattack. Brazil's law number 9,983 of 2000 criminalizes the unauthorized alteration of computer data. Canada's Criminal Code Section 342.1 criminalizes most forms of cyberattacks. Denmark's Penal Code Section 263 criminalizes unauthorized access to computer information and programs. France's Penal Code Article 323-1 criminalizes the fraudulent access of computer systems. Germany's Penal Code criminalizes the unauthorized access or modification of computer data, and damaging a computer system. India's Information Technology Act of 2000 criminalizes computer hacking. Japan's Unauthorized Computer Access Law of 1999 criminalizes most forms of cyberattacks. The Netherlands Penal Code Article 138 criminalizes the unauthorized access of a computer system. South Africa's Electronic Communications and Transactions Act of 2002 criminalizes cybercrime. Switzerland's Penal Code Article 143bis criminalizes the authorized access of computer data. The United States and United Kingdom both have robust criminal laws against cyberattacks, basically criminalizing all forms of them. *See id.* at 17–22, 40–42, 175–184. Many other states have criminalized computer crimes, such as the unauthorized access or alteration of data, or computer sabotage, but those laws shall not be covered in this paper. Garnett & Clarke, *supra* note 13, at 471.

State responses to transnational terrorist attacks further support recognition of a duty to prevent cyberattacks under CIL. After the 9/11 terrorist attacks, states across the world condemned terrorism as a threat to international peace and security, and provided various forms of support to the United States in its war against Al Qaeda.[398] Ensuring that terrorism will forever be legally recognized as a threat to international peace and security, the Security Council passed Resolution 1373, which reaffirmed that acts of international terrorism were threats to international peace and security, and called on states to work together to prevent and suppress terrorism.[399] The resolution further directed states to "refrain from providing any form of support" to terrorists through act or omission, to "deny safe haven" to those who commit terrorist acts, and "afford one another the greatest measure of assistance in connection with criminal investigations . . . [or] proceedings" related to terrorism.[400] While the international community's response to terrorism does not directly define CIL regarding cyberattacks, it is persuasive on several fronts. First, it shows that states have a duty to prevent threats to international peace and security. Second, it demonstrates that passive acquiescence to threats to international peace and security will not be tolerated. Finally, it demonstrates that states must work together to prevent and suppress threats to international peace and security. Because states are growing more dependent on computer systems connected to the internet,[401] and cyberattacks are increasing in both frequency and

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

[399] S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

[400] *Id.*, ¶ 1.

[401] *See supra* Part I.A; *supra* Part II.B.

potency,[402] there should be little doubt that cyberattacks are a growing threat to international peace and security. The more cyberattacks resemble terrorism, the more easily they'll fit into the paradigm constructed to deal with transnational terrorism. However, no matter what purpose cyberattacks are used for, they represent a threat to international peace and security, and should be dealt with similarly to other recognized transnational threats.

Numerous U.N. declarations about international crime also support recognition of the duty to prevent cyberattacks as described in this section. These declarations urge states to take affirmative steps to prevent non-state actors from using their territory to commit acts that cause civil strife in another state.[403] Furthermore, these declarations also support the duty of states to cooperate with one another to eliminate transnational crime, which lends credence to the duty to cooperate with victim-states during the criminal investigation and prosecution of cyberattacks.[404]

[402] *See supra* Part I.A; *supra* Part II.B.

[403] The 1970 Declaration on Friendly Relations urges states to "refrain from . . . acquiescing [to] organized activities within [their] territory directed towards the commission of [civil strife or terrorism in another state]." G.A. Res. 2625, *supra* note 283, ¶ 1. The 2000 Vienna Declaration on Crime and Justice states that "We [must] commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime." 2000 Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century, G.A. Res. 55/59, Annex, ¶ 18, U.N. Doc. A/RES/55/59/Annex (Jan.17, 2001). The 2001 Draft Articles of State Responsibility require states to affirmatively take action to uphold their international duties to other states, including those arising from CIL, and declare that when states fail to act, they may be held indirectly responsible for such inaction. Draft Articles on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/CN.4/L.602/Rev. 1 (2001).

[404] The 1970 Declaration on Friendly Relations notes that "States have a duty to cooperate with one another . . . in order to maintain international peace and security." G.A. Res. 2625, *supra* note 283, ¶ 1. The 2004 Report of the High-Panel on Threats, Challenges and Change recognizes the growing threat of organized transnational crime as a threat to international peace and security, stating that "today, more than ever, threats are interrelated and a threat to one is a threat to all." The Secretary-General, *Report of the High-Panel on Threats, Challenges and Change*, ¶ 17, *delivered to the General Assembly*, U.N. Doc A/59/565 (Dec. 2, 2004). It goes on to further state:

> No State, no matter how powerful, can by its own efforts alone make itself invulnerable to today's threats. Every State requires the cooperation of other States to make itself secure. It is in every State's interest, accordingly, to cooperate with other states to address their most

Focusing specifically on cyberattacks, states have both made declarations themselves, and used the U.N. General Assembly to make numerous declarations about the importance of preventing cyberattacks. For instance, the U.N. General Assembly has called on states to criminalize cyberattacks,[405] and to deny the territory of its member-states from being used as a safe haven to conduct cyberattacks through state practice.[406] The General Assembly has also called on states to cooperate with each other during the investigation and prosecution of international cyberattacks.[407] Even China has said it will "take firm and effective action to prevent all hacking attacks that threaten computer systems."[408] Furthermore, states are starting to recognize the threat that cyberattacks pose to international peace and security, with some states and the General Assembly directly recognizing cyberattacks as a danger to international peace and security.[409] These declarations all evidence recognition that the duty

> pressing threats, because doing so will maximize the chances of reciprocal cooperation to address its own threat priorities.

Id., ¶ 24.

[405] G.A. Res. 45/121, ¶ 3, U.N. Doc. A/RES/45/121 (Dec. 14, 1990) (embracing the principles adopted by the Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, and inviting states to follow them); G.A. Res. 55/63, ¶ 1, U.N. Doc. A/RES/55/63 (Jan. 22, 2001); *see also* Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, Aug. 27–Sept. 7, 1990, *report prepared by the Secretariat*, at 140–43, U.N. Doc. A/CONF.144/28/Rev.1 (1991).

[406] G.A. Res. 55/63, *supra* note 405, ¶ 1.

[407] G.A. Res. 45/121, *supra* note 405, ¶ 3 (embracing the principles adopted by the Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, and inviting states to follow them); G.A. Res. 55/63, *supra* note 405, ¶ 1; *see also* Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, Aug. 27–Sept. 7, 1990, *report prepared by the Secretariat*, at 140–43, U.N. Doc. A/CONF.144/28/Rev.1 (1991).

[408] McGregor & Williamson, *supra* note 44 (quoting China's Premier Wen Jiabao's pledge to prevent international cyberattacks in response to allegations that China is ignoring international cyberattacks).

[409] *See* THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003) (noting the threat that cyberattacks pose to international peace and security); Convention on Cybercrime, *supra* note 23 (recognizing cyberattacks as a threat to international peace and security and calling on states to work together to end the cyberthreat); Huw Jones, *Estonia Calls for EU Law to Combat Cyberattacks*, REUTERS, Mar. 12, 2008, http://www.reuters.com/ article/reutersEdge/idUSL1164404620080312 (reporting Estonia's call to fight

of states to prevent cyberattacks as a matter of CIL also includes the following lesser duties: passing stringent criminal laws, vigorously investigating cyberattacks, prosecuting attackers, and having the host-state and victim-state cooperate during the investigation and prosecution of cases.

3. *Support from the General Principles of Law*

The general principles of law common to civilized nations also support recognition of a duty to prevent cyberattacks. It is a well-established principle under the domestic laws of most states that individuals should be responsible for acts or omissions that have a causal link

cyberattacks as a threat to international peace and security); G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (Jan. 4, 1999) (noting that information technology can affect the interests of the entire international community; expressing concern that information technology can be used to disrupt international stability; and noting that it is necessary for states to stop information technology from being used for criminal or terrorist purposes); G.A. Res. 54/49, ¶ 2, U.N. Doc. A/RES/54/49 (Dec. 23, 1999) (considering it necessary to prevent the use of information technology to be used for criminal or terrorist purposes, and recommending states develop international principles to combat cybercrime and cyberterrorism); G.A. Res. 55/28, U.N. Doc. A/RES/55/28 (Dec. 20, 2000) (recognizing that the misuse of information technology can be a threat to international stability, and urging states to cooperate to eliminate the misuse of such technology); G.A. Res. 56/19, U.N. Doc. A/RES/56/19 (Jan. 7, 2002) (reaffirming the conclusions of General Assembly Resolutions 53/70, 54/49, and 55/28); G.A. Res. 56/121, U.N. Doc. A/RES/56/121 (Jan. 23, 2002) (noting increased state cooperation to combat criminal misuse of information technology; noting the necessity of preventing the criminal misuse of information technology; underlining the need to continue to increase state cooperation against the criminal misuse of information technology; and urging states to continue to work to eliminate the criminal misuse of information technology); G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Dec. 30, 2002); G.A. Res. 57/239, ¶ 1–5, U.N. Doc. A/RES/57/239 (Jan. 31, 2003) (calling on states to “create a global culture of cybersecurity”); G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 18, 2003); G.A. Res. 58/199, ¶ 1–6, U.N. Doc. A/RES/58/199 (Jan. 30, 2004) (recognizing the threat that cyberattacks pose to CNI; recognizing that protecting CNI requires international cooperation and law enforcement; and calling on states to create a global culture of cybersecurity); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 16, 2004); G.A. Res. 59/220, ¶ 4, U.N. Doc. A/RES/59/220 (Feb. 11, 2005) (endorsing the Declaration of Principles adopted at the 2003 World Summit on the Information Society, *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html, which recognizes the need for states to prevent information technology from being used for criminal or terrorist purposes); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Jan. 6, 2006); G.A. Res. 60/252, ¶ 8, U.N. Doc. A/RES/60/252 (Apr. 27, 2006) (reiterating the need for states cooperation); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 19, 2006); *see also* G.A. Res. 51/210, ¶ 3, U.N. Doc. A/RES/51/210 (Dec. 16, 1996) (calling upon states “to note the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and the need to find means, consistent with national law, to prevent such criminality and to promote cooperation where appropriate”); S.C. Res. 1373, *supra* note 399, ¶ 3 (calling upon states to cooperate and share information about the “use of communication technology by terrorist groups”).

to the harm suffered by another individual.[410] While international law is not obligated to follow the domestic laws of states,[411] international law may be "derived from the general principles common to the major legal systems of the world."[412] Since most states use causation as a principle for establishing individual responsibility, it lends credence to the principle that states responsibility should also be based on causation. Thus, if a state failed to pass stringent criminal laws, did not investigate international cyberattacks, or did not prosecute attackers, it should be held responsible for international cyberattacks against another state because its omission helped create a safe place for attackers to attack other states. Furthermore, the general duty to prevent attacks already accounts for causation to some degree,[413] which lends credence to using causation analogies from domestic laws when interpreting the customary duty to prevent attacks insofar as it applies to cyberattacks.

4. Support from Judicial Opinions

[410] BECKER, *supra* note 310, at 285–86. Causation is applied differently by states. Some states use a 'but for' test, looking to see whether the harm in question "would have occurred were it not for the conduct in question." *Id.* at 291. Other states use a 'proximate cause' test, looking to see whether harm was reasonably foreseeable as a result of an individual's actions or omissions. *Id.* Omissions are generally treated the same as acts. So, for instance, if a parent chose not to feed his/her child, the parent would still bear responsibility for the harm to the child because their failure to act caused harm when it was their duty to prevent such harm. *Id.* at 294–97.

[411] *Id.* at 287.

[412] RESTATEMENT, *supra* note 289, § 102.

[413] For instance, in *Corfu Channel Case*, the ICJ held that Albania was responsible for notifying British ships of a minefield in their waters, even though the mines were laid by non-state actors, because it was unreasonable to assume that Albania did not know of their presence (even though Albania claimed not to know of them), and because states have a duty to prevent their territory from being used to harm other states when it is within their power to do so. In effect, Albania could have prevented the British ships from hitting the mines, but their failure to act caused the British ships harm. *See* Corfu Channel Case (Merits), 1949 I.C.J. 4 (Apr. 9). *But see* BECKER, *supra* note 310, at 287–89 (noting that some scholars argue that international law and domestic law are so dissimilar that comparisons between the two are useless).

Finally, judicial opinions further support recognition of a state's affirmative duty to prevent cyberattacks from its territory against other states. In *Tellini*, a special committee of jurists held that a state may be held responsible for the criminal acts of non-state actors when it "neglect[s] to take all reasonable measures for the prevention of the crime and pursuit, arrest and bringing to justice of the criminal."[414] In *S.S. Lotus*, the Permanent Court of International Justice (ICJ) held that "a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people."[415] In *Corfu Channel Case*, the ICJ held that states have a duty "not to allow knowingly its territory to be used for acts contrary to the rights of other states."[416] While these are older cases, the principles in the cases still stand for and lend support to the notion that states have a duty to prevent their territory from being used to commit criminal acts against another state, as well as the duty of states to pursue, arrest and bring to justice criminals who have conducted cross-border attacks on other states.

5. Further Defining a State's Duty to Prevent Cyberattacks

A state's duty to prevent cyberattacks should not be based on a state's knowledge of a particular cyberattack before it occurs, but rather on its actions to prevent cyberattacks in general. Cyberattacks are extremely difficult for host-states to detect prior to the commission

[414] *Tellini* case, 4 League of Nations O.J. 524 (1924).

[415] *See* S.S. Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 4, 88 (Moore, J., dissenting).

[416] Corfu Channel Case (Merits), 1949 I.C.J. 4, 22 (Apr. 9).

of a specific attack,[417] and are often committed by individuals or groups who aren't even on a state's radar. However, just because cyberattacks are difficult to prevent, does not mean that states cannot breach their duty to prevent them. Stringent criminal laws and vigorous law enforcement will deter cyberattacks.[418] States that fail to enact such laws fail to live up to their duty to prevent cyberattacks through passiveness and indifference. Likewise, even when a state has stringent criminal laws on the books, if it looks the other way when cyberattacks are conducted against rival states, it effectively breaches its duty to prevent cyberattacks through its unwillingness to do anything to stop the cyberattacks, just as if it had approved them.[419] In other words, a state's passiveness and indifference toward cyberattacks make it a sanctuary state, where attackers can safely launch attacks. When viewed in this light, it becomes apparent that a state can be held indirectly responsible for cyberattacks under the established principles of CIL.

D. Becoming a Sanctuary State: Practices that Lead to State Responsibility

The question of whether a state is acting as a sanctuary state is extremely fact dependent. When considering this question, victim-states must look at the host-state's criminal laws, law enforcement practices, and track record of cooperating with the victim-

[417] *See* Naraine, *supra* note 171 (referencing Secretary of Homeland Security Michael Chertoff's speech on the vulnerability of federal computer systems).

[418] *See* COLARIK, *supra* note 6, at 39; KAMAL, *supra* note 23, at 176.

[419] States that are unable to fulfill their duty to prevent cyberattacks, due to the lack of technical expertise, should be viewed in compliance with its duty to prevent them when it accepts technical assistance from the victim-state to hunt down the attackers who attacked it. Cooperating in law enforcement efforts demonstrates their willingness to prevent cyberattacks. Whereas, states that lacked the technical expertise to hunt attackers, but who refused to accept outside assistance, would be viewed as unwilling to take the necessary steps to bring attackers to justice.

states of cyberattacks that previously originated from inside its borders. In effect, host-states will be judged on their efforts to catch and prosecute attackers who have committed cyberattacks, which is probably the only way that states can deter and prevent future attacks. Since victim-states will end up judging whether a host-state has lived up to its international duties, host-states must cooperate with victim-states to ensure transparency. Cooperation will necessarily entail a host-state showing its criminal investigations to a victim-state, so victim-states can correctly judge host-state action. Furthermore, when a host-state lacks the technical capacity to track down an attacker, the law should require it to work together with law enforcement officials from the victim-state to jointly track down the attackers.[420] These two measures will prevent host-states from being perceived as uncooperative and complicit in the use of their networks for attacks against other states. States that deny involvement in a cyberattack, but refuse to open their investigative records to the victim-state, end up casting doubt on their willingness to stop cyberattacks and cannot expect to be treated as a state living up to its international duties. In effect, host-states that refuse to cooperate with victim-states are unwilling to prevent cyberattacks and have declared themselves a sanctuary state.

Once a host-state demonstrates that it is a sanctuary state through inaction, other states can impute responsibility to it. At that point, it becomes liable for the cyberattack that triggered an initial call for investigation, as well as all future cyberattacks originating from it. This opens the door to a victim-state to use active defenses against the computer servers in that state during a cyberattack.

[420] This position is supported by numerous United Nations General Assembly Resolutions, the European Convention on Cybercrime, and other United Nations documents, which all generally urge states to cooperate in investigating and prosecuting the criminal misuse of information technologies. *See supra* notes 391, 403–07, 409 and accompanying text; UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER RELATED CRIME ¶ 268–73 (1995), *available at* http://www.uncjin.org/Documents/irpc4344.pdf.

VI. The Choice to Use Active Defenses: Why States Should Use Active Defenses, and the Challenges States Will Encounter During *Jus ad Bellum* and *Jus in Bello* Analysis Due to the Limits of Technology

When states choose, as a matter of policy, to forcibly respond to armed cyberattacks, their responses must comply with both principal areas of the law of war—*jus ad bellum* and *jus in bello*.[421] While this paper contends that active defenses are the most appropriate response under the law of war, readers should not take this as a given without justification. Theoretically, once one accepts that states may legally respond to cyberattacks in self-defense or anticipatory self-defense, the necessary consequence is that states may use force to the extent authorized under *jus in bello*. Therefore, unless *jus in bello* stops states from using conventional force, forcible responses are not limited to active defenses. Furthermore, while this paper's primary focus is to justify the use of active defenses, states that choose to use active defenses will find that their ability to analyze cyberattacks is challenged by the limits of technology. This will complicate state *jus ad bellum* and *jus in bello* analysis at both the highest and lowest levels of state decision-making. State decision-makers will need to account for these limitations when making state policy. System administrators will need to account for these limitations when responding to actual cyberattacks.

This part will analyze these issues. First, it will analyze the technological limitations that are likely to affect state *jus ad bellum* analysis. Next, it will move on to the *jus in bello* issues. *Jus in bello* analysis will begin with the decision to use force, analyzing why active defenses are the most appropriate *jus in bello* response to cyberattacks. Finally, *jus in bello* analysis will conclude with the impact that technological limitations are likely to have on

[421] *See supra* notes 174–75 and accompanying text.

state decisions to use force. Once this is complete, it will be clear that active defenses are a viable way for states to protect themselves despite the fact that technological limitations will complicate state decision-making.

A. Technology Limitations and *Jus ad Bellum* Analysis

While cyberattack analysis is greatly simplified by looking at whether a state of origin has violated its duty to prevent, rather than having to attribute an attack, states are still likely to find cyberattacks difficult to deal with in practice. *Jus ad bellum* requires states to carefully analyze a cyberattack and ensure that: (1) the attack constitutes an armed attack or imminent armed attack; and (2) the attack originates from a sanctuary state. Both of these conditions must exist before a state can lawfully respond with active defenses under *jus ad bellum*.

Cyberattack analysis will be conducted by system administrators, whose position puts them at the forefront of computer defense. System administrators can use various computer programs to facilitate their analysis. Automated detection and warning programs can help detect intrusions, classify attacks, and flag intrusions for administrator action.[422] Automated or administrator-operated trace programs can trace attacks back to their point of origin.[423] These programs can help system administrators to classify cyberattacks as armed attacks or

[422] *See* Naraine, *supra* note 171 (referencing a speech by former Secretary of Homeland Security Michael Chertoff, in which he described the Einstein program, which the federal government uses to protect its computer systems).

[423] *See* Wheeler & Larsen, *supra* note 162, at 23–24 (discussing the use of automated tracer programs to find the originating point of a cyberattack). *See generally* Wheeler & Larsen, *supra* note 162 (for a technical discussion on tracing cyberattacks back to their point of origin).

lesser uses of force, and evaluate whether attacks originate from a state previously declared a sanctuary state by state decision-makers. When attacks meet the appropriate legal thresholds, system administrators may use active defenses to protect their networks.[424]

Unfortunately, technological limitations on attack detection, attack classification and attack traces are likely to further complicate state decision-making during cyberattack analysis. Ideally, attacks would be easy to detect, classify and trace. However, this is not the case. This section will analyze the technological limits of these programs and explore their likely impact on state decision-makers and system administrators.

1. Limitations on Attack Detection

While early detection and warning programs can help catch cyberattacks before they reach their culminating point, even the best programs are unable to detect all cyberattacks.[425] As a result, cyberattacks are bound to harm states. From a legal perspective, the failure to catch an attack until after its completion has both an upside and a downside. On the upside, states would gain the luxury of time to evaluate an attack, since the threat of danger will have already passed. On the downside, tracing an attack back to its source becomes more difficult the farther removed the trace becomes from the time of attack.[426] Furthermore, even when it

[424] *See supra* Part III.C–D (discussing the thresholds for armed attacks and imminent armed attacks); *supra* Part V.A (discussing cyberattacks as armed attacks); *supra* Part V.B–C (discussing state responsibility for cyberattacks when states violate their duty to prevent them); *see also* Wheeler & Larsen, *supra* note 162, at 24 (noting that the U.S. Department of Defense has already developed these capabilities, but has been restricted from using them by the U.S. Department of Justice due to the legal issues that active defenses raise).

[425] *See* Naraine, *supra* note 171 (quoting former Secretary of Homeland Security Michael Chertoff).

[426] *See* Wheeler & Larsen, *supra* note 162, at 51–52. An ongoing attack is the easiest form of cyberattack to trace back to its source, allowing states to trace an electronic pathway back to the source. *Id.* at 9–42, 51–52. Completed attacks are much more difficult to trace, since the electronic pathways no longer exist, data may be

turns out that an armed cyberattack originates from a sanctuary state, state decision-makers would need to think long and hard about using active defenses as a matter of law and policy. The longer it takes to detect an attack, the less compelling the need for states to use active defenses, especially when the attack seems truly complete. On the other hand, when an attack that has reached completion is seen as part of a series of ongoing attacks, the need to use active defenses to deter future attacks is more compelling.[427]

2. Limitations on Attack Classification

Early detection and warning programs will detect many cyberattacks mid-attack. However, detecting an attack before its culmination makes it harder to classify. Naturally, a system administrator will immediately attempt to shut down a cyberattack with passive defenses as soon as it's detected. However, that is not the full extent of his job. The system administrator must also assess the damage that's been done, as well as any likely future damage, so that an informed decision can be made about whether to use active defenses.[428]

destroyed, and piercing the shield that zombies or other intermediaries create for the true attacker (assuming intermediaries were used) becomes more difficult once an attack has already been completed. *Id.* at 51–52.

[427] The more an attack is seen as part of a series of attacks originating from the host-state, the more extensive a victim-state's response can be. This will be highly fact dependent, based on behavioral trends of the host-state and intelligence about the host-state's intentions. *See supra* Part III.C–D. Thus, cyberattacks from sanctuary states are more likely to be seen as part of an ongoing series of attacks, even when the attacks are actually committed by different attackers within the state, because they've already demonstrated that they allow attacks to come from them unchecked. *See supra* Part V.B–C.

[428] System administrators must determine whether the attack meets the threshold of an armed attack. To do so, they'd need to weigh: (1) the potential harm that could occur from the attack to ensure that it was an armed attack; (2) the likelihood of fending off the attack with purely defensive measures, to ensure that active defenses were necessary; and (3) the imminency of such harm, since active defenses may not be employed until delaying their use starts to endanger the state. These decisions will, no doubt, be based on rules promulgated by the victim-state before the attack ever occurs. These rules would simplify the legal framework into a set of rules more easily understood by the layman, similar to the rules of engagement that military personnel follow.

When an ongoing cyberattack has already caused severe, invasive and measurable damage, it can safely be classified as an armed attack, even though it is still ongoing.[429] On the other hand, when an attack has not caused severe, invasive or measurable damage, a system administrator will need to look at the immediacy of future harm to determine whether the attack should be classified as an imminent armed attack.[430] Given the lightning speeds with which computer codes can execute, this will be very difficult to do, as delaying the use of active defenses increases the likelihood of harm to a state.[431]

The limitations on attack classification should give system administrators pause before deciding to use active defenses in anticipatory self-defense. While it is lawful to make a decision based on their best analysis of the facts ,[432] such determinations will be highly

[429] *See supra* Part V.A. A good example of an ongoing attack that had already risen to the level of an armed attack when it was detected was the 2007 cyberattack against Estonia. In those attacks, the cyberattack no doubt rose to the level of an armed attack early in the process, disrupting the ability of the Estonian government to govern; yet the attacks continued on for several weeks afterwards, further damaging Estonian systems far beyond the damage at the point of detection. *See supra* Part I.A.

Furthermore, when evaluating a cyberattack as an armed attack, it is also important to determine whether a cyberattack is part of a series of coordinated cyberattacks against a state. When this happens, it is possible for the collective effect of the attacks to rise to the level of an armed attack, even though none of the individual attacks did so. In this type of situation, cyberattacks against non-critical infrastructure can be considered an armed attack based on their collective effect. *See supra* Part V.A. This would require analysis at a higher national level than the institution being individually attacked, but might be possible with government coordination. The Cyber Warning and Information Network and National Cyber Alert System is an example of such an effort in the United States. *See* WILSON, *supra* note 15, at CRS-31 to CRS-32. The 2007 cyberattacks against Estonia were an example of a coordinated set of cyberattacks that collectively rose to the level of an armed attack. While some of the attacks on Estonia were against critical infrastructure, and might have been armed attacks anyway, the collective effect was much greater than the damage done in any of the individual attacks, and certainly pushed those cyberattacks to the level of armed force. *See supra* Part I.A.

[430] *See supra* Part V.A.

[431] System administrators can attempt to quarantine and analyze malicious code to buy time. However, this is not always possible. Furthermore, unauthorized remote penetrations cannot be quarantined or slowed down. For these cyberattacks, system administrators will need to sever the connection and end the attack, which may not always be possible. However, all of this takes time, which is why it is easier to automate classification and trace programs to uncover the basic facts about a cyberattack and its point of origin, flag the attack for a system administrator’s attention, and have active defenses at the ready. *See supra* Part II.C.

[432] *See supra* note 375 and accompanying text.

speculative due to the shadowy nature of cyberattacks. Most likely, when a computer intrusion is detected, the purpose of the attack will be extremely difficult to discern without taking time to dissect a program's code or review the audit logs of an attacker's activity.[433] Furthermore, the speed with which cyberattacks execute will force system administrators to make their best guess, even though they'll probably be missing critical information. Given the speculative nature of any such calculus,[434] as a matter of policy, state decision-makers may want to tell their system administrators to respond to cyberattacks in anticipatory self-defense only as an act of last resort to prevent an escalation of hostilities between states.

3. Limitations on Attack Traces

Cyberattacks are frequently conducted through intermediate computer systems to disguise the true identity of an attacker.[435] While trace programs are capable of penetrating intermediate disguises back to their electronic source, their success rate is not perfect.[436]

[433] For instance, the purpose of malware may range from collecting information, to testing a state's defenses, to launching a full scale attack. Furthermore, since remote penetrations are conducted by individuals, the purpose of the attack may be impossible to know without questioning the attacker.

[434] Using active defenses in anticipatory self-defense will undoubtedly come under intense international scrutiny the first few times it happens, and anger the host-state whose borders were electronically crossed. While states may legally act in anticipatory self-defense when it appears that an armed attack is imminent, it must be prepared to be questioned by other states who do not agree with its analysis. Ultimately the state's actions will be judged using the Rendulic Rule from a legal perspective, and in the court of public opinion from a diplomatic perspective. Thus, anticipatory self-defense should only be used when a state feels that an after-the-fact analysis will truly support its actions. *See supra* note 375 and accompanying text.

[435] *See* WILSON, *supra* note 15, at CRS-5 to CRS-7 (discussing the use of zombie computer systems to disguise the identity of an attacker); Ruth Wedgwood, *Proportionality, Cyberwar, and the Law of War, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 219, 227–30 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002) (discussing the use of looping and weaving to disguise the identity of an attacker). *See generally* Wheeler & Larsen, *supra* note 162 (discussing the technical methods of using intermediary computer systems to disguise the source of a cyberattack).

[436] *See generally* Wheeler & Larsen, *supra* note 162 (discussing the technical capabilities of trace programs).

Thus, trace programs run the risk of incorrectly identifying the true source of an attack. This creates an apparent problem because an attack could be incorrectly perceived as coming from a state that is not the actual state of origin. However, this is not as big a problem as it appears. State responsibility should still be judged on the facts at hand, even if it results in a misattribution. The reason that misattribution is not a problem is twofold. First, as long as a state assesses an attack to the best of its technical capability and acts in good faith on the information on hand, it has met its international obligations.[437] Second, states that refuse to comply with their international duty to prevent their territory from being used to commit cyberattacks have chosen to risk being held indirectly responsible by accident. After all a state can avoid being the target of active defenses, even when attacks originate from it, by taking affirmative steps to prevent cyberattacks, such as enacting stringent criminal laws, enforcing those laws, and cooperating with victim-states to bring attackers to justice.

B. *Jus in Bello* Issues Related to the Use of Active Defenses

Decisions about what type of force a state should use are governed by *jus in bello*. *Jus in bello* generally stands for the proposition that the "right of belligerents to select methods and means of warfare is not unlimited."[438] At its core, *jus in bello* uses five basic

[437] *See supra* note 375 and accompanying text.

[438] Brown, *supra* note 52, at 198. This principle is derived from Hague Convention IV, Annex, Article 22, which states, "[t]he right of belligerents to adopt means of injuring the enemy is not unlimited." Hague Convention IV Respecting the Laws and Customs of War on Land and its Annex (Regulations), Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague IV].

principles to regulate the conduct of belligerents during warfare.[439] These are the principles of distinction, necessity, humanity, proportionality and chivalry.[440]

1. *Active Defenses, the Most Appropriate* Jus in Bello *Response*

[439] The number of core principles of *jus in bello* varies per source. While sources disagree on the number of core principles, all agree that the five principles listed here are fundamental tenets of *jus in bello*. The disagreement is merely over which principles are "core" and which are lesser principles. *See* COMMANDER'S HANDBOOK, *supra* note 60, § 5.3, 12.1.2 (identifying four core principles of *jus in bello*, but listing a fifth principle to follow); Brown, *supra* note 52, at 185 (identifying five core principles of *jus in bello*); WINGFIELD, *supra* note 49, at 131 (identifying four core principles of *jus in bello*, but noting a fifth "subsidiary" principle).

[440] *See* COMMANDER'S HANDBOOK, *supra* note 60, § 5.3, 12.1.2 (identifying four core principles of distinction, necessity, humanity and proportionality, but later listing perfidy (also known as chivalry) as a fifth principle to follow); Brown, *supra* note 52, at 185; WINGFIELD, *supra* note 49, at 131 (identifying four core principles of distinction, necessity, proportionality and chivalry, but noting that humanity is a subsidiary principle).

Distinction "is the requirement to distinguish combatants and military objectives from noncombatants . . . and civilian objects, and to attack only the former." WINGFIELD, *supra* note 49, at 131. This principle is derived from Additional Protocol I, Article 48, which states, "[p]arties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]. However, distinction doesn't protect civilians who directly participate in hostilities. *Id.*, art. 51(3).

Necessity limits the amount of force a state can use against legitimate targets "to that required for mission accomplishment and force protection," and forbids using force purely "for the sake of destruction." WINGFIELD, *supra* note 49, at 131.

Humanity prohibits the use of weapons designed to cause unnecessary suffering. WINGFIELD, *supra* note 49, at 131. This principle is derived from Hague Convention IV, Annex, Article 23, which states, "it is especially forbidden . . . to cause unnecessary suffering." Hague IV, *supra* note 438.

Proportionality protects civilians and their property the same way necessity and humanity protect lawful targets from excessive uses of force. WINGFIELD, *supra* note 49, at 154. Understanding that attacks on legitimate targets will often cause incidental damage beyond the lawful target itself, proportionality limits the use of force to situations in which the expected military advantage outweighs the expected collateral damage to civilians and their property. WINGFIELD, *supra* note 49, at 154–55. This principle is derived from Additional Protocol I, Article 51(5)(b), which states that it is prohibited to use force that "is 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 440.

Chivalry prohibits states from abusing the law of war to gain military advantages over their adversaries. WINGFIELD, *supra* note 49, at 159–72. This principle is derived from Additional Protocol I, Article 37, which states, "[i]t is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe he is entitled to, or is obligated to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy." Additional Protocol I, *supra* note 440.

While the focus of this paper is justifying the use of active defenses in response to cyberattacks, once one accepts that states are legally authorized to respond to cyberattacks in self-defense or anticipatory self-defense, the necessary consequence is that states may use force to the extent authorized under *jus in bello*.[441] In other words, unless *jus in bello* stops states from using conventional force, states can legally use other weapons in response to cyberattacks. Therefore, it is worth explaining why state decision-makers should choose to use active defenses, as a matter of policy, as the most appropriate response to cyberattacks.

Active defenses are the most appropriate type of force to use against cyberattacks in light of the principles of *jus in bello*. There are several reasons for this. First, in terms of military necessity, active defenses probably represent all the force needed to accomplish the mission of defending against a cyberattack. Active defenses can trace an attack back to its source and immediately disrupt it; whereas kinetic weapons will be slower and less effective than the lightning speed of a hack-back.[442] Therefore employing kinetic weapons over active defenses will not only be less effective, but will also violate the principle of necessity by employing force purely for destruction's sake. Second, in terms of proportionality, active defenses are less likely to cause disproportionate collateral damage than kinetic weapons. The traceback capabilities of active defenses allow them to target only the source of a cyberattack.[443] While collateral damage may still result because the originating computer server serves multiple functions, unless an attacker uses CNI to conduct the attack, damage

[441] *See supra* note 175 and accompanying text.

[442] *See supra* Part II.C (discussing defenses to cyberattacks).

[443] *See supra* Part II.C (discussing the capabilities of active defenses); Wheeler & Larsen, *supra* note 162, at 23–24 (discussing the use of automated tracer programs to find the originating point of a cyberattack). *But see infra* Part VI.A.3 (discussing the limitations of trace programs).

should be fairly limited from the use of active defenses. Furthermore, since the majority of cyberattacks are conducted by non-state actors,[444] it seems unlikely that many attacks will come from CNI.[445] Thus, active defenses provide states a way to surgically strike at their attacker with minimal risks of severe collateral damage to the host-state;[446] meeting the proportional requirement "to select [the] method or means of warfare likely to cause the least collateral damage and incidental injury, all other things being equal."[447] Finally, while not stemming from *jus in bello*, choosing active defenses over kinetic weapons should reduce the chance of escalating these situations into full scale armed conflicts between states.

2. Technological Limitations and Jus in Bello *Analysis*

Unfortunately, despite the increased security that active defenses provide, using them is not without legal risk. Technological limitations may prevent states from conducting the

[444] *See* Jensen, *supra* note 26, at 232.

[445] However, when cyberattacks originate from critical systems the host-state bears responsibility for allowing them to be used in such a manner because states have an obligation to police their own citizens. *See supra* Part IV.B. By failing to do so, states declare themselves sanctuary states and give other states the legal grounds to respond in self-defense to cyberattacks from them. *See supra* Part IV.C–D. The principle of discrimination requires states to segregate their civilian objects from military objects. *See* Jensen, *supra* note 375, at 1174 (referencing Additional Protocol I, Article 58). Thus, the host-state is effectively responsible for the collateral damage that occurs because it has allowed attackers within its territory to mix their means of attack with civilian objects, making them dual use in nature and legitimate subjects of attack. *See* Michael Schmitt, *Wired Warfare: Computer Network Attack and the Jus in Bello*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 187, 198–99 (Michael N. Schmitt & Brian T. O'Donnell eds., Naval War College 2002).

[446] *See* Jensen, *supra* note 375, at 1174 (noting that active defenses can be designed to simply shut a computer off to stop an attack, rather than permanently disabling it); Schmitt, *supra* note 445, at 204–05 (arguing that active defenses may simply shut down computer systems for a brief time, rather than having to use kinetic weapons, which inherently cause physical destruction to achieve their objectives). *But see* Wedgwood, *supra* note 435, at 227–30 (arguing that it is harder to confine the effects of active defenses than it is with kinetic weapons because the links from a computer to the civilian infrastructure it controls are less apparent).

[447] Schmitt, *supra* note 445, at 204.

surgical strikes envisioned with active defenses.[448] The more an attacker routes his attack through intermediary systems, the more difficult it is to trace the attack.[449] Furthermore, complex traces take time, which isn't always available during a moment of crisis.[450] Adding to these difficulties, trace programs often have problems pinpointing the source of an attack once an attacker terminates his electronic connection.[451] Sometimes these difficulties will simply result in a failure to identify the source of an attack, other times it may result in the incorrect identification of an intermediary system as the source of an attack.[452] Even when the source of an attack is correctly identified, the victim-state's system administrator must map out the attacking computer system to distinguish its functions and the likely consequences that will result from shutting it down.[453] The problem is that system mapping takes time, often more time than a state has to make an informed decision.[454] Sometimes a system will be able to be mapped quickly, allowing states to make informed decisions about likely collateral damage. Other times a state will be forced to try to predict the likely consequences of using active defenses without having fully mapped a system. As a result,

[448] *See* Wedgwood, *supra* note 435, at 227–30 (arguing that there isn't enough time to properly map the functions of an attacking computer system when using active defenses, which may result in counter-strikes having broader than intended consequences).

[449] *See generally* Wheeler & Larsen, *supra* note 162 (discussing ways to trace cyberattacks to their source).

[450] *See* Wedgwood, *supra* note 435, at 227–30.

[451] *See generally* Wheeler & Larsen, *supra* note 162 (discussing ways to trace cyberattacks to their source).

[452] *See* Wedgwood, *supra* note 435, at 227–30 (noting that looping and weaving techniques may cause faulty traces); WILSON, *supra* note 15, at 5–7 (noting that zombies are often used to conduct cyberattacks). *See generally* Wheeler & Larsen, *supra* note 162 (discussing ways to trace cyberattacks to their source).

[453] *See* Barkham, *supra* note 30, at 82–83; Jensen, *supra* note 460, at 1184–85.

[454] *See* Wedgwood, *supra* note 435, at 227–30.

any state that employs active defenses runs the risk of accidentally targeting innocent systems and causing unintended excessive collateral damage.[455]

To ensure the lawful use of active defenses in accordance with the principles of distinction and proportionality, states must do "everything feasible" to mitigate these risks.[456] In the realm of active defenses, this means doing everything feasible to identify: (1) the computer system that launched the initial attack; and (2) the probable collateral damage that will result from using active defenses against that system.[457] Once a state does everything feasible to ensure it has the right information and acts in good faith in accordance with *jus in bello*, it is legally protected from erroneous calculations, even when it targets civilian

[455] *See* Barkham, *supra* note 30, at 82–83; Jensen, *supra* note 375, at 1178–79. Targeting innocent systems violates the principle of distinction, unless it meets the safe harbor of the Rendulic Rule. Jensen, *supra* note 375, at 1178–86. Causing excessive collateral damage in relation to the military advantage gained violates the principle of proportionality, unless it meets the safe harbor of the Rendulic Rule. *Id*.

[456] Jensen, *supra* note 375, at 1183–86. This principle is derived from Additional Protocol I, Article 57(2), which states:

> (a) those who plan or decide upon an attack shall:
>
> (i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects . . . ;
>
> (ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;
>
> (iii) refrain from deciding to launch any 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 440.

[457] *See* Jensen, *supra* note 375, at 1183–86. It is important to note that probable consequences are judged as the consequences that "'may be expected,' not what is likely or possible, or even what is foreseeable." *Id.* at 1179. *See generally* Brown, *supra* note 52, at 198–202 (discussing the requirements of distinction, necessity, humanity and proportionality regarding cyberattacks).

systems or causes excessive collateral damage in relation to its military objective.[458] "The important point is that a [state] is required only to do what is feasible, given the prevailing circumstances, including the time [it] has to make a decision and the amount of information it has during that time."[459] Thus, states may still act with imperfect information, based on the way facts appear at the time, when the potential danger forces them to act; [460] the real test will be whether danger to the victim-state's systems justified the use of active defenses in light of the likely collateral damage to the host-state.[461]

While beyond the scope of this paper, there are several issues worthy of consideration before a state decides to implement active defenses. First, due to the compressed timelines of cyberattacks, a state may need to automate its active defenses so that it can respond to cyberattacks in a timely manner. However, utilizing automated defenses will increase the likelihood of violating the principles of distinction and proportionality. As a result, defenses should probably only be automated for detection purposes, requiring human analysis and approval before actually counter-striking. Second, just because it is legal to use active defenses under the circumstances described in this paper, does not mean it is sound policy. States must decide whether the diplomatic fallout is worth the risk. Unfortunately, technological limitations can cause state calculations to be erroneous at times, and cause civilian systems to be targeted or excessively damaged. States must decide that the second guessing which other states will engage in is worth the benefit gained from protecting their

[458] *See* Jensen, *supra* note 375, at 1184–86 (discussing the legal protection granted to states and decision-makers under the Rendulic Rule).

[459] *Id.* at 1186.

[460] *See id.* at 1183.

[461] *See* Brown, *supra* note 52, at 201–02.

computer systems. Third, there is the chance that the servers from which the initial attacks originate are intimately tied to important systems in the host-state, which if turned off could have devastating effects and cause unnecessary suffering. This possibility must be factored into the state's evaluation of military necessity versus probable collateral damage, especially if a state responds with active defenses without fully mapping an attacking system. Fourth, states should carefully design their active defenses. Poorly coded active defense programs run the risk of self-propagating in cyberspace, beyond their initial purpose, and can run the risk of evolving from a defensive program into a computer virus or worm, whose damage goes far beyond its intended design. Since active defenses represent a new frontier in cyberwarfare, their initial use will be controversial, no matter the situation. States should expect public scrutiny and diplomatic protests until such time as active defenses are recognized as a lawful method of self-defense under international law.

VII. Conclusion

Cyberattacks are one of the greatest threats to international peace and security in the twenty-first century. Securing cyberspace is an absolute imperative. In an ideal world, states would work together to eliminate the cyberthreat. Unfortunately, our world is no utopia; nor is it likely to become one. Sanctuary states refuse to cooperate with other states to eliminate cyberattacks. The attitude of sanctuary states casts doubt on reaching a global international agreement to secure cyberspace at any time in the near future. Perhaps one day global cooperation to eliminate cyberattacks will be a reality. However, unless something changes to pressure sanctuary states into changing their behavior, there is no impetus for them to do so. As a result, states must seek other solutions to address the current cyberthreat, and coerce sanctuary states into fulfilling their international duty to prevent cyberattacks.

The way to achieve this reality is to hold sanctuary states responsible for violating their duty to prevent cyberattacks and use active defenses against cyberattacks originating from within their borders. Not only will this allow victim-states to protect themselves from cyberattacks, but it should push sanctuary states into taking their international duty seriously. After all, no state wants another state using force within its borders, even electronically. Thus, the possibility of a forceful response to cyberattacks within their borders is the hammer that can drive some sense into sanctuary states.

Since states do not currently use active defenses, any decision to use them will be a controversial and scary change to state practice. Like any proposal that changes the way states do business, this proposal is bound to be met with criticism on a number of fronts.[462] However, there is sound legal authority to use active defenses against states that violate their

[462] The largest critiques are likely to come from those who believe that: (1) cyberattacks are not acts of war and should be treated as a criminal matter; or (2) victim-states should have to prove that a state initiated the cyberattack or exercised directed control over the attacker before it is allowed to use active defenses. However, some critics are even likely to critique this paper's approach as not going far enough to protect state CNI from cyberattacks because it prevents states from using active defenses when attacks are not from sanctuary states.

Critics who argue that cyberattacks cannot rise to the level of armed attacks miss the way the law has responded to unconventional attacks in the past. Furthermore, these critics also miss an important facet of international law—reprisals, which can be used as an alternate basis to authorize active defenses against cyberattacks. *See supra* notes 359, 377 and accompanying text.

Critics who argue that this paper goes too far by advocating for the use of active defenses without having to prove a state's involvement in the attacks miss the way that the law of state responsibility has evolved over the past thirty-years. Their arguments rest on the prevailing view of state responsibility for cyberattacks, which is rooted in outdated understandings of the law. *See supra* Part I.B (discussing the response crisis); *supra* Part IV.C (analyzing the law of state responsibility); V.B (analyzing state responsibility for cyberattacks).

Critics who argue that the approach advocated by this paper does not go far enough to protect state CNI, and advocate using strict liability as the legal standard to protect CNI, miss a crucial part of the legal analysis—namely, just because CNI is under armed attack does not give a victim-state legal authority to violate the territorial integrity of the host-state. *See supra* notes 355, 361, 386 and accompanying text.

duty to prevent cyberattacks. When this paper is reviewed, and the authorities it relies on carefully analyzed, it is obvious that states have an affirmative duty to prevent cyberattacks.[463] States that violate this duty, and refuse to change their practices, should be held responsible for all further attacks originating from within their borders in accordance with the law of war.[464] At a time when cyberattacks threaten global security, and states are scrambling to find ways to improve their cyberdefenses,[465] there is no reason to shield sanctuary states from the lawful use of active defenses by victim-states, and every reason to enhance state defenses to cyberattacks by using them.

[463] *See supra* Part V.C (discussing the duty to prevent cyberattacks under CIL).

[464] Today, state responsibility for the actions of non-state actors results from a state's failure to live up to their international duties to other states with respect to those non-state actors. *See supra* Part IV.C. This includes the duty to prevent cyberattacks. *See supra* Part V.B–C.

[465] During former President George W. Bush's administration, the United States initiated a $30 billion cyberdefense plan to protect government computer networks from attack. Since President Obama has taken office, he has identified cybersecurity as one of the most important national security concerns of the United States, and has ordered a review of U.S. cyberdefenses to find ways to improve cybersecurity. The review of U.S. cyberdefenses is still ongoing at the time of this paper's submission. However, in one of the reports already prepared for the President, one of the recommendations is to reexamine the law regarding military responses to cyberattacks. *See* Keith Epstein, *U.S. is Losing Global Cyberwar, Commission Says*, BUSINESSWEEK.COM, Dec. 7, 2008, http://www.businessweek.com/bwdaily/dnflash/content/dec2008/db2008127_817606.htm; Peter Eisler, *Raids on Federal Computer Data Soar; 'Major Intrusions' on Networks are Up 40%*, USA TODAY, Feb. 17, 2009, at 1A; Byron Acohido, *Obama Taps Cybersecurity Expert to Assess U.S. Defenses*, USA TODAY, Feb. 17, 2009, at 8B; Byron Acohido, *White House Urged to Stop Cyberattacks*, USA TODAY.COM, Mar. 11, 2009, http://blogs.usatoday.com/technologylive/2009/03/the-united-stat.html; CENTER FOR STRATEGIC AND INT'L STUD. COMMISSION ON SECURING CYBERSPACE FOR THE 44TH PRESIDENCY, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 8 (2008) (recommending to the President to direct the Attorney General to reexamine the law, and "issue guidelines as to the circumstances and requirements for the use of . . . [the] military . . . in cyber incidents").