Cyber Attacks and the Legal Justification for an Armed Response

A Monograph

by

MAJ Joshua A. Mendoza
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-03-2017	Master's Thesis	JUN 2016 – MAY 2017

4. TITLE AND SUBTITLE
Cyber Attacks and the Legal Justification for an Armed Response

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Joshua A. Mendoza

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Operational Arts Studies Fellowship, Advanced Military Studies Program.

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

When is an armed response to cyber attacks legally justified? International law does not refer to cyber, cyber attack targets, or the effects of a cyber attack in the same manner that it addresses conventional attacks, target selection, and effects. Cyber attacks are certainly not a new phenomenon and have been a growing threat for more than thirty years, resulting in the current potential for causing catastrophic harm. Existing sources of international law sufficiently provides the legal justification required for armed response despite not directly using cyber terminology. The analysis provided in this monograph addresses the need for clarification of the legal and political justification for armed response to a cyber attack. Political leaders must have the legal justification for armed response but must also mitigate political risk. This monograph proposes policy factors to be used to decide whether armed response that is legally justifiable is warranted. Political leaders need to determine the likelihood of attack, and look at the effects of multiple types of scenarios, not just the worst case.

15. SUBJECT TERMS
Cyber; Cyber attack; Cyber act of war; Use of force; Armed attack; Armed response; Act of agression; Act of violence; Legal justificaiton; Legal guidelines; Policy; Severity, Casualties; Immediacy; Attribution; Politics; Specificity; Intent

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Major Joshua A. Mendoza
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	41	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Monograph Approval Page

Name of Candidate: Major Joshua A. Mendoza

Monograph Title: Cyber Attacks and the Legal Justification for Armed Response

Approved by:

_____, Monograph Director
Melissa Thomas, PhD

_____, Seminar Leader
Jason J. McGuire, COL

_____, Director, School of Advanced Military Studies
James C. Markert, COL

Accepted this 25th day of May 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernandez, PhD

Abstract

Cyber Attacks and the Legal Justification for Armed Response, by MAJ Joshua A. Mendoza, US Army, 41 pages.

When is an armed response to cyber attacks legally justified? International law does not refer to cyber, cyber attack targets, or the effects of a cyber attack in the same manner that it addresses conventional attacks, target selection, and effects. Cyber attacks are certainly not a new phenomenon and have been a growing threat for more than thirty years, resulting in the current potential for causing catastrophic harm. Existing sources of international law sufficiently provide the legal justification required for armed response despite not directly using cyber terminology. The analysis provided in this monograph addresses the need for clarification of the legal and political justification for armed response to a cyber attack. Political leaders must have the legal justification for armed response but must also mitigate political risk. This monograph proposes policy factors to be used to decide whether armed response that is legally justifiable is warranted. Political leaders need to determine the likelihood of attack, and look at the effects of multiple types of scenarios, not just the worst case.

Contents

Acknowledgement

I would like to express my sincere gratitude to my monograph director, Dr. Melissa Thomas, PhD, for her guidance and dedication throughout the course of this effort. I would also like to thank my Seminar Leader, COL Jason “Jay” McGuire, for keeping me “on the bus.” Most of all, I would like to acknowledge the love and support of my wife Ashley, and my daughters Isabella and Mckenna, for their understanding that monograph time meant less family time. Each of you has always been and will always be critical to my success.

Acronyms and Terms

AUMF	Authorized Use of Military Force
CNA	Computer Network Attack
Cyberspace	A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
DDOS	Distributed Denial of Service
DoD	Department of Defense
Domain	An area owned, controlled, or contested by a ruler or government such as land, sea, air, space or cyber
FEMA	Federal Emergency Management Agency
ICJ	International Court of Justice
IHL	International Humanitarian Law
LOAC	Law of Armed Conflict
LOW	Law of War
NATO	North Atlantic Treaty Organization
NATO CCDCOE	North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence
NIST	National Institute of Standards and Technology
STUXNET	Malicious computer worm designed to attack specific uranium enrichment machines in Iran
UN	United Nations
US	United States
USCYBERCOM	United States Cyber Command
Zero-Day Vulnerability	Opening in software that is unknown to original creative vendor

Tables

Introduction

The single biggest existential threat that's out there, I think, is cyber.

—ADM(R) Michael Mullen

When is an armed response to cyber attacks legally justified? This question arises from a lack of understanding of what constitutes a cyber attack, what legal and political justification is required for an armed response, and who makes that determination. International law does not refer to cyber, cyber attack targets, or the effects of a cyber attack in the same manner that it addresses conventional attacks, target selection, and effects.

Cyber attacks are certainly not a new phenomenon and have been a growing threat for more than thirty years, resulting in the current potential for causing catastrophic harm (i.e. digital Pearl Harbor). The growing threat of cyber attacks has led to a demand for clarification of the permissibility of armed response. The *Cyber Act of War Act* legislation introduced to Congress by Senator Mike Rounds in May of 2016 is an example of the demand for clarification. The *Cyber Act of War Act* calls for "the development of a policy for determining when an action carried out in cyberspace constitutes an act of war against the United States."[1]

The focus on whether cyber attacks are "acts of war" is misplaced and creates a perception that the United States will respond to a cyber attack with a declaration of war. A declaration of war is only one, and not the most commonly used, form of armed response. Armed response for cyber attacks is more likely to occur as an Authorization for the Use of Military Force (AUMF) since formal declarations of war have fallen out of favor. Since World War II, the preferred method of armed response from the United States is an AUMF, a form of response that

[1] Scott Maucione, "Senator Wants Definition on Cyber Act of War," Federal News Radio, May 9, 2016, accessed September 22, 2016, http://federalnewsradio.com/cybersecurity/2016/05/senator-wants-definition-cyber-act-war/.

dates back to 1798. Another implication of the bill is that current international law does not provide adequate guidance for armed response to cyber attacks. In fact, the existing legal framework of international law is sufficiently applicable to an armed response to cyber attacks and was purposely written to be broad enough to incorporate new concepts, technology, and terminology.

The analysis provided in this monograph addresses the need for clarification of the legal and political justification for armed response to a cyber attack. Understanding when an armed response to cyber attacks is legally justified begins with understanding the various definitions of cyber attack. Simultaneously describing the circumstances of the growing cyber problem demonstrates how the history of cyber attacks has led to demands for the clarification of the permissibility of an armed response. Existing sources of international law provide the legal justification required for armed response despite not directly using cyber terminology. A comparison of how cyber attacks conform to the language used to define conventional attacks further supports the claim that existing law is sufficient. An analysis of current cyber policy demonstrates that the United States considers existing international law sufficient, offering additional support for the sufficiency of current law. This monograph proposes policy factors to be used to decide whether armed response that is legally justifiable is warranted. Finally, hypothetical illustrations provide what-if scenarios that are outside the norms of conventional attacks to which existing international law and the proposed factors for decisions can be applied to determine if an armed response is legally justified and politically advisable.

The Need for Clarification of the Definition of a Cyber Attack

Understanding when an armed response to cyber attacks is legally justified begins with understanding the various definitions of cyber attack. There are currently fifteen definitions of

"cyber attack" used by the international community.[2] As cyber attacks have increased in intensity and frequency, they are now meeting multiple definitions of cyber attack and creating the potential for catastrophic harm (i.e. digital Pearl Harbor). The historical illustrations of cyber attacks reveal the reasoning behind the call for clarification of the legality of armed response. Although the *Cyber Act of War Act* legislation introduced in May 2016 appears justified, it is asking the wrong question.

A cyber action must be considered a "cyber attack" before further analysis of whether an armed response is legally justified. The North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence (NATO CCDCOE) provides a glossary of terms that attempts to clarify how different nations and organizations interpret and define cyber terminology to include "cyber attack," of which there are fifteen definitions.

This monograph refers to the two definitions of cyber attack most relevant to the United States. The 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare* (the Tallinn Manual) contains the opinions of legal and cyber experts that constitute a source of international law.[3] The Tallinn Manual contains ninety-five black letter rules covering topics that include *jus ad bellum* (right to war), *jus in bello* (how wars are fought), sovereignty, treaty, and customary law and applies to both state and non-state actors. The Tallinn Manual definition of "cyber attack" is one definition referenced in this monograph.[4] The US definition of "cyber attack" is the other definition used. This definition, written in May of 2013, comes from the

[2] NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), "Cyber Definitions," accessed May 5, 2017, https://www.ccdcoe.org/cyber-definitions. The following countries or sources have provided definitions of cyber attack: Austria, Canada, Germany, Lithuania, North Atlantic Treaty Organization (NATO), New Zealand, National Institute of Standards and Technology (NIST), Oxford Dictionary, United States, Tallinn Manual, Russia, Switzerland, Romania, Nigeria, and the United Kingdom.

[3] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), 1.

[4] Ibid., 106.

National Institute of Standards and Technology (NIST) working underneath the US Department of Commerce.[5] Table 1 shows the source, definition, and applicability of the definitions used in this monograph:

Table 1. Definitions and Applicability to Cyber Attack

Source	Definition	Applicability
United States	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information	Applies only to domestic attacks; limited in scope and effect to digital systems; does not address civilian casualties
Tallinn Manual	A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects	Applies to domestic and international attacks; not limited in scope and effect where catastrophic harm exists

The wording of the definitions may create the misunderstanding that a cyber attack that meets the Tallinn Manual definition does not fall under the US definition. In fact, the US definition is set at a lower threshold so a catastrophic cyber attack satisfies both of them.

The description of historical cyber actions that follows applies the term "cyber attack" to actions that happened prior to the development of formal definitions of "cyber attack" in order to show the linkage between attack and legal justification. The history of cyber attacks goes back over thirty years and as attacks have grown more intense, they have ultimately met several definitions of cyber attack, providing the justification for armed response.

[5] Richard Kissel, "Glossary of Key Information Security Terms," *NIST Interagency Reports NIST IR* 7298, no. 3 (2013), 57, accessed February 25, 2017, https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/NIST.IR.7298r2.pdf. "The NIST has received numerous requests to provide a summary glossary for our publications and other relevant sources, and to make the glossary available to practitioners."

The legal terminology used to evaluate whether a provocation justifies an armed response includes "use of force," "armed attack," "act of aggression," or "act of violence." These terms are used interchangeably depending on the source. The most advisable determination of legal justification for an armed response to a cyber action follows three steps. First, the action is determined to be a "cyber attack" using the definitions stated in Table 1. Second, a "cyber attack" must qualify as a "use of force" (a "use of force" qualification does not necessarily constitute legal justification for armed response). Third, with further analysis, the "use of force" is determined to be an "armed attack." Unfortunately, the process does not always happen in this manner. For instance, upon further analysis of a cyber attack that qualifies as a "use of force," use of the terms "act of aggression" or "act of violence" may replace "armed attack," which may not assist in determining legal justification for armed response. Additionally, "act of aggression" and "act of violence" can replace "use of force," thus requiring further clarification of the legal justification for an armed response.

The first discovered cyber threat against the United States took place in the US Embassy in Moscow and the US Consulate in Leningrad from 1976 to 1984. (An attack on an embassy is an attack on the country it represents).[6] In an espionage operation referred to by US officials as "Project Gunman," Soviets incorporated keystroke logging hardware on IBM Selectric typewriters newly installed in the embassy and consulate for day-to-day business, classified letters, and official memoranda.[7] The stealing of information occurred over an eight-year span from 1976 to 1984 in which Soviets were able to utilize listening devices tuned to television frequencies to avoid detection, transmitting keystroke information in sixteen typewriters from the

[6] Discover Diplomacy, "What Is a U.S. Embassy?" accessed October 25, 2016, https://diplomacy.state.gov/discoverdiplomacy/diplomacy101/places/170537.htm.

[7] Dan Goodin, "How Soviets Used IBM Selectric Keyloggers to Spy on United States Diplomats," Ars Technica, October 13, 2015, accessed August 21, 2016, http://arstechnica.com/security/2015/10/how-soviets-used-ibm-selectric-keyloggers-to-spy-on-us-diplomats/.

embassy and the consulate to listening stations across the street. This qualifies as a cyber attack under the US definition as it was designed to steal controlled information.

The first attack on a military network occurred in February of 1998. The attack, which US officials named “Operation Solar Sunrise,” focused on gaining access to military computers at Andrews Air Force Base in Washington, DC in order to roam the network.[8] This attack was hard to detect because it was a network intrusion designed to pull information rather than destroy the system. Once found, technicians later discovered that this intrusion was not an isolated event. This hack had spread to over a dozen more installations including the Pentagon. Deputy Secretary of Defense John Hamre warned that this could be "the first shots of a genuine cyberwar" initially thought to be originating in Iraq (although incorrect, Deputy Secretary of Defense Hamre's words foreshadowed events to come). Ultimately, agents discovered that two sixteen-year-old US citizens working in concert with an eighteen-year-old Israeli hacked into these networks. While this hack does not fit the US definition of a “cyber attack,” it did demonstrate what could be done to a military network not properly secured.

The "love bug" virus originating in the Philippines in May 2000 infected nearly 50 million US computers, shutting down mail servers across the world.[9] The United States demanded extradition of the culprits and had an existing extradition law with the Philippines. The Philippines, however, did not have a law against hacking and did not extradite the perpetrators of the computer network attack (CNA). This attack meets the US definition of cyber attack by maliciously controlling the email network in order to disrupt and disable it. It is unresolved whether this attack ultimately “damaged” the network. To satisfy the Tallinn Manual definition,

---

[8] Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016), 73-78.

[9] Armando A. Cottim, “Cybercrime, Cyberterrorism, and Jurisdiction. An Analysis of Article 22 of the Coe Convention on Cybercrime,” in *Law and Technology: Looking into the Future: Selected Essays*, ed. Meritxell Fernández-Barrera et al. (Florence: European Press Academic Publishing, 2009), accessed December 15, 2016, http://www.ejls.eu/6/78UK.htm.

"damage" would have to be interpreted as the complete loss of access to email servers; until such time as the servers could be repaired and brought back online.

On April 27, 2007, Estonia, a North Atlantic Treaty Organization (NATO) member, was hit by a massive cyber distributed denial of service (DDOS) attack, allegedly by Russia, which caused the shutdown of networks and servers supporting 1.3 million Estonians.[10] These networks controlled all aspects of life in the state including banking, ATM, telephones, personal networks, government networks, and military communications. For nearly a month, almost all digital access in Estonia shut down. Estonia considered this cyber attack a cyber act of war. Ene Ergma, the speaker of the Estonian parliament, stated, "Like nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything."[11] The Estonia cyber action meets the US definition of cyber attack.

The Estonia attack is the first instance of an international cyber attack testing the effectiveness of Article 5 of the North Atlantic Treaty of 1949. Under Article 5, each NATO member agrees that an armed attack on one is an attack on all. If such an attack occurs, then each member state pledges to come to the aid of the requesting state but a complete NATO consensus of the twenty-eight members is required for action.[12] The North Atlantic Treaty does not explicitly define what constitutes an armed attack. NATO as a collective organization has not given a definition of an armed attack. In the sixty-seven year history of NATO, requested Article 5 aid was granted only once, following the 9/11 terrorist attacks.[13] The entire effectiveness of

---

[10] Kaplan, *Dark Territory*, 162-165.

[11] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *WIRED*, August 21, 2007, accessed January 26, 2017, https://www.wired.com/2007/08/ff-estonia/.

[12] *North Atlantic Treaty*, Art. 5, 34 U.N.T.S. 243, August 24, 1949.

[13] NATO, "Collective Defence - Article 5," accessed January 26, 2017, http://www.nato.int/cps/en/natohq/topics_110496.htm. On the evening of September 12, 2001, less than 24 hours after the attacks, and for the first time in NATO's history, the Allies invoked the principle of Article 5. Then NATO Secretary General Lord Robertson subsequently informed the Secretary-General of the United Nations of the Alliance's decision.

NATO may be called into question if an Article 5 request was not met with action despite having near consensus.

However, Estonia's requested aid under Article 5 was denied for two reasons. First, NATO did not reach consensus that the cyber action met the threshold for an armed attack. An article in the *NATO Legal Gazette* did state that "measures that result in significant physical damage to objects, or injury or death to a person can thus be considered uses of force. Measures that only cause loss of data or financial loss are not uses of force."[14] This is very similar to the Tallinn Manual definition of cyber attack. Second, Estonia did not provide conclusive evidence of attribution to support the claim that Russia initiated the attack. In this case, NATO determined that this cyber attack caused a loss of data and financial loss but did not constitute a use of force, let alone an armed attack.

According to some (including Estonia's foreign minister Urmas Paet), the Estonia attack allegedly perpetrated by Russia appears to have been a dress rehearsal for an attack occurring a year later in a campaign against Georgia to annex South Ossetia and Abkhazia.[15] Russian cyber attacks occurred simultaneously with physical land and air crossings of international borders. Over fifty Georgian websites' traffic rerouted to Russian servers that promptly shut down all web traffic and activity, causing disruption in nearly every sector of life. The digital shutdown included traffic generated from government and military communication systems, banking systems, and media outlets. The Georgia cyber attack meets the Tallinn Manual definition satisfying the clause "reasonably expected to cause injury or death to persons, or damage or

[14] Pascal Brangetto, Tomas Minárik, and Jan Stinisson, "From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications," *NATO Legal Gazette*, no. 35 (December 2014): 20.

[15] Catherine A. Theohary and Anne I. Harrington, *Cyber Operations in DOD Policy and Plans: Issues for Congress* (Washington, DC: Congressional Research Service, 2015), 10, accessed October 25, 2016, https://pdfs.semanticscholar.org/73f1/5e0fb26f8ad007d1f8257651fd04f45691e8.pdf.

destruction to objects."[16] A reasonable person would expect that causing disruption to military systems and first responder networks could lead to injury or death.

The 2010 STUXNET attack on Iranian nuclear centrifuges that deliberately destroyed uranium enrichment capability and shut down nearly 1000 centrifuges at the Natanz nuclear plant was the first purely cyber attack that had damaging and lasting physical effects. In 2012, the *New York Times* reported this was a joint venture between the United States and Israel.[17] As sophisticated as this attack was, with revolutionary malware designed to seek and destroy a single target, it still had unintended effects. A Belarussian cybersecurity analysis of replicating malware occurring on Microsoft Windows operating systems led to the discovery of the STUXNET attack, which had spread outside the intended target.[18] This attack meets the definition of a cyber attack for both the United States and the Tallinn Manual and demonstrates that cyber attacks are increasing in intensity to the point of possible catastrophic harm.

Recent computer network attacks against critical infrastructure in the United States have increased to the point that warrants higher levels of concern. The Industrial Control System Cyber Emergency Response Team reported two hundred and ninety-five cyber incidents involving critical infrastructure in 2015, an increase of fifty events from 2014.[19] As the technology that attackers use continues to improve, the potential for catastrophic harm grows on a daily basis. The effects of cyber attacks are critical to the legal justification of an armed response.

---

[16] CCDCOE, "Cyber Definitions."

[17] David E. Sanger, "Obama Ordered Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, accessed January 26, 2017, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[18] Theohary and Harrington, *Cyber Operations in DOD Policy and Plans*, 11.

[19] Davis, "Hackers Take Down the Most Wired Country in Europe."

International attacks on Estonia, Georgia, and Iran, along with attacks on United States critical infrastructure, inspired Senator Mike Rounds to introduce the bill *Cyber Act of War Act* on May 5, 2016. The bill provides:

> (a) POLICY REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the President shall—
>
> (1) develop a policy for determining when an action carried out in cyberspace constitutes an act of war against the United States; and
>
> (2) revise the Department of Defense Law of War Manual accordingly.
>
> (b) CONSIDERATIONS.—In developing the policy required by subsection (a)(1), the President shall consider the following:
>
> (1) The ways in which the effects of a cyber attack may be equivalent to the effects of an attack using conventional weapons, including with respect to physical destruction or casualties.
>
> (2) Intangible effects of significant scope, intensity, or duration.[20]

The submission of this bill was the first time that Congress formally introduced legislation requesting the definition for an "act of war," cyber or otherwise. As of March 18, 2017, the Senate Committee on Foreign Relations has been reviewing the bill since May 9, 2016. An identical bill submitted to the House of Representatives Armed Services Committee was referred to the Subcommittee on Emerging Threats and Capabilities on June 7, 2016, where is currently still sits.[21]

The bill is asking the wrong question. The question whether an action in cyberspace constitutes an act of war is misplaced. Calling a cyber attack an "act of war" has dire consequences, as it commits the United States to armed conflict and armed response may not be politically expedient. The question should be "when is an armed response to cyber attack legally

[20] *Cyber Act of War Act of 2016*, S. 2905, 114th Cong., 2nd Sess. (2015-2016), accessed October 25, 2016, https://www.congress.gov/bill/114th-congress/senate-bill/2905/text.

[21] *Cyber Act of War Act of 2016*, H.R. 5220, 114th Cong. (2015-2016), accessed October 21, 2016, https://www.congress.gov/bill/114th-congress/house-bill/5220/actions.

justified?" This particular question removes the necessity of an automatic armed response and only asks whether legal justification for armed response exists.

Legal Guidelines

US domestic law does not provide legal justification for an armed response to a cyber attack. However, Title 18 of the US Code defines an "act of war," limited to a specific context, and is included so the reader understands that domestic law was considered. The central question here is how cyber attacks relate to the existing framework and terminology of international law when presented in the proper context. International law is broad enough to incorporate new concepts, technology, and terminology. The United States, NATO, and the Tallinn Manual agree that existing international law is sufficient to address the justification of an armed response to a cyber attack. However, the law dealing with armed response uses a number of poorly defined terms, namely "use of force," (no authoritative definition exists)[22] "armed attack," "act of aggression," and "act of violence." Additionally, several sources of international law contain multiple uses of these terms and appear to use them interdependently or interchangeably at times.

A sole definition of an "act of war," cyber or otherwise, exists within domestic law. Title 18, Section 2331 states that an act of war is "any act occurring in the course of (A) declared war; (B) armed conflict, whether a war has been declared or not; (C) armed conflict between military forces of any origin."[23] The definition above applies only to Title 18, Chapter 113B "Terrorism," and is not applicable beyond the context of terrorism. Applying this definition to cyber attacks outside the context of terrorism will not provide legal justification for armed response and is more applicable to discussing cyber attacks in the context of *jus in bello* (how wars are fought). "*Jus in bello* provisions apply to the warring parties irrespective of the reasons for the conflict and

[22] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* 46.

[23] 18 U.S.C., § 2331 (2012), accessed October 4, 2016, http://uscode.house.gov/.

whether or not the cause upheld by either party is just."[24] Since the reason for conflict does not matter under *jus in bello* principles, the legal justification of armed response cannot be determined. US domestic law does not address the question of whether an armed response to a cyber attack is legally justified, so the analysis looks to international law for answers.

Article 38 of the International Court of Justice (ICJ), the principal judicial agent of the United Nations (UN), describes the four sources of international law as:

> a. international conventions (treaties), whether general or particular, establishing rules expressly recognized by the contesting states;
>
> b. international custom, as evidence of a general practice accepted as law;
>
> c. the general principles of law recognized by civilized nations;
>
> d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.[25]

The sources of international law referenced in this monograph include ICJ judgments and opinions, the UN Charter, UN General Assembly resolutions, The Tallinn Manual, the Law of Armed Conflict (LOAC), The Geneva Conventions, The Hague Conventions, and the Budapest Convention.

Some in the international community have concerns about the applicability of existing law towards cyber since, at the time of establishment of our current legal norms, cyber threats were not a concern.[26] "International cyber security law is not a legal term of art," meaning there is no legal definition because case law, treaty or customary law directly relating to cyber warfare does not exist.[27] There is a disagreement amongst experts as to the definition of the word "armed"

---

[24] International Committee of the Red Cross (ICRC), *IHL and Other Legal Regimes-Jus Ad Bellum and Jus in Bello*, accessed December 15, 2016, https://www.icrc.org/eng/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm.

[25] Statute of the International Court of Justice, art. 38, ¶ 1, accessed September 22, 2016, http://www.icj-cij.org/documents/?p1=4&p2=2#CHAPTER_II.

[26] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 3.

[27] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 14.

and whether cyber actions can constitute an "armed attack" due to a lack of employed "weapons" in the conventional understanding. However, the twenty experts who co-authored the Tallinn Manual unanimously agree that the existing sources of international law apply to cyber attacks and can legally justify armed response. The ICJ's judgment in *Nicaragua v.United States of America* and its opinion in *Nuclear Weapons Advisory* make apparent that, although cyber law does not exist, existing law is sufficient for cyber attacks and refute the claim that an armed attack cannot occur due to a lack of employed weapons. In addition, the most recent US cyber policy document, President Obama's 2011 *International Strategy for Cyberspace,* makes clear that existing sources of international law are applicable to cyber in the following strategy statement:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace.[28]

Some sources of international law contain a specific clause to cover unforeseen circumstances, which would include the growing cyber threat. If a cyber attack occurs which is not explicitly covered under international law, the Martens Clause found in the Geneva Conventions[29] and the Preamble to the Hague Convention IV[30] ensure that an armed response may still be legally justified. The Martens Clause states:

---

[28] President of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, 2011), 9, accessed December 15, 2016, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

[29] Cornell University of Law, *Geneva Conventions*, August 6, 2007, accessed December 15, 2016, https://www.law.cornell.edu/wex/geneva_conventions.

[30] Yale Law School, "Laws of War: Laws and Customs of War on Land (Hague IV); October 18, 1907," accessed December 15, 2016, http://avalon.law.yale.edu/20th_century/hague04.asp#art54.

> Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience.

The Martens Clause exists to ensure that activities such as cyber are not conducted in a legal vacuum.[31] The legal experts who have written the *Tallinn Manual* note that if an expressed rule of customary law does not account for cyber actions, the Martens Clause takes precedence. Existing law that does not mention cyber explicitly is therefore interpreted as sufficient until such a time that the law is rewritten.

The loosely defined terms used in international law such as "use of force," "armed attack," "act of aggression," and "act of violence," are used interdependently or interchangeably creating potential confusion in their use, leading to the question of how these terms relate to cyber attacks. Using the language that describes conventional attacks, a cyber attack may be determined to be a use of force, and further, can qualify as an armed attack. Building on the *Nicaragua* judgment of 1986, cyber attacks qualify as an armed attack and armed response is justified when the "scale and effects" of the attack amount to the scale and effect of attacks from conventional forces.[32] The *Nicaragua* judgment explicitly references the UN General Assembly Resolution 3314 (XXIX) (Definition of Aggression) to assist in determining whether an action qualifies as "use of force" and an "armed attack," citing the resolution as reflecting customary law. The determination must distinguish the "most grave forms" of use of force (those that amount to an armed attack) from other less grave forms, although it is not stated how to draw this distinction.

---

[31] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 77-78.

[32] "Military and Paramilitary Activities in and against Nicaragua" (Nicaragua v. United States of America), Judgment, 1986 I.C.J. Rep. 14, ¶ 191 and 195 (June 27).

The *Nuclear Weapons Advisory Opinion* of 1996 holds that the method and means of attack are of no concern in determining whether an operation qualifies as an armed attack.[33] The opinion points to the fact that the UN Charter neither prohibits nor allows specific weapons. The logic of this opinion applies to cyber attacks because the means and employment of a cyber attack are immaterial to the determination that the attack constitutes a use of force and on further analysis, may qualify as an armed attack.

The Tallinn Manual answers the question of whether a cyber attack can be considered an armed attack if it meets certain criteria. A cyber action is not an armed attack if the scale and effects are not comparable to conventional actions rising to the level of a use of force.[34] The Tallinn Manual considers the following factors to determine if a cyber action is a use of force rising to the level of an armed attack: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[35] The authors reference the *Nicaragua* judgment and the *Nuclear Weapons Advisory Opinion* when discussing their factors for determining the difference between use of force and armed attack applicable to cyber attacks. According to the Tallinn Manual, no cyber incidents since 2012 have reached the threshold of an armed attack.[36] Even the historical attacks previously mentioned that many, at initial glance, might consider an armed attack, such as the cyber attack on Estonia in 2007, Russia's cyber attack on Georgia in 2008, and the United States and Israel's STUXNET attack on Iran in 2010 did not reach the threshold the Tallinn Manual lays out.

---

[33] "Legality of the Threat or Use of Nuclear Weapons," Advisory Opinion, 1996 I.C.J. Rep. 226, ¶. 39 (July 1996).

[34] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 45. The Tallinn Manual states that there is no authoritative definition of, or criteria for, "threat" or "use of force" in any source of legal authority despite the prevalence of the use of terms.

[35] Ibid., 48-52.

[36] Ibid., 57.

The Law of Armed Conflict (LOAC) also known as the Law of War (LOW), and International Humanitarian Law (IHL) are the "customary and treaty law applicable to the conduct of warfare on land and to relationships between belligerents and neutral States."[37] Four principles constitute the LOAC. They are military necessity, proportionality, distinction, and unnecessary suffering. The Tallinn Manual states that the LOAC applies to cyber operations as it would any other operation of a conventional nature, but limitations to applicability exist.[38] The Tallinn Manual states that the LOAC did not apply to attacks in Estonia because the situation did not rise to the level of an armed conflict, where armed conflict is defined as "a situation involving hostilities, including those conducted using cyber means." The effects of the Estonia attack did not rise to the level of use of force, let alone an armed attack, whereas the attack on Georgia a year later did. The Tallinn Manual states that the definition of armed conflict was met in the Georgia attack because cyber actions were conducted in furtherance of the conflict along with conventional attacks. Even if a cyber attack does not meet the threshold for an "armed attack," legal justification for an armed response may exist citing the LOAC principle of unnecessary suffering if a cyber attack grossly violates the Geneva or Hague Conventions where methods of warfare, which would include cyber, that cause superfluous injury or unnecessary suffering are prohibited.[39]

The United Nations Charter uses several interdependent, undefined terms ("use of force," "armed attack," and "acts of aggression") that lead to debates about the legal justification for armed response. The primary purpose of the UN Charter, established in June of 1945, stated in Article 1, is to maintain international peace and suppress acts of aggression or other breaches of

---

[37] *International and Operational Law Department, Law of Armed Conflict Deskbook* (Charlottesville, VA: The Judge Advocate General's Legal Center and School, 2012), 8.

[38] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare, 75-78.*

[39] *International and Operational Law Department, Law of Armed Conflict Deskbook,* 149.

the peace.[40] Article 2(4) states that all nations shall refrain from the threat or use of force against another state.[41] The UN Charter does not provide any criteria to determine when an act amounts to a use of force, act of aggression, or an armed attack.[42]

Chapter VII (Articles 39-51) of the UN Charter applies specifically to threats, breaches of the peace, acts of aggression, and armed attack. [43] Article 39 states that the UN Security Council determines if an act of aggression exists. While the Charter does not explicitly reference the UN General Assembly Resolution 3314 (XXIX) (Definition of Aggression), an offended nation would need to reference it to determine whether an act of aggression occurred. Article 41 lists actions that could be considered a use of force that do not justify an armed response. "These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations." Article 42 states that if the Security Council were to deem any proportional response measures, short of armed response, against those interruptions previously outlined in Article 41 as inadequate, armed response is then authorized to restore international peace. Although not specifically included, this would include cyber attacks by implication. Article 51 of the Charter states "that nothing present in the Charter itself will inhibit the right of an individual state to self-defense if an armed attack occurs." Response measures may be taken immediately, if reported to the UN Security Council, by the offended nation. The nation must later prove the attack qualified as an armed attack.

---

[40] United Nations, *Charter of the United Nations*, Art. 1, accessed August 21, 2016, http://www.un.org/en/charter-united-nations/.

[41] Ibid., Art. 2, ¶ 4.

[42] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 45.

[43] United Nations, *Charter of the United Nations*, Articles 39-42, 51.

The term "use of aggression" is defined in the UN General Assembly's Resolution 3314 (XXIX) (Definition of Aggression). The UN General Assembly is one of the six principal organs of the UN established in its Charter.[44] A primary function of the UN General Assembly is to provide resolutions and recommendations. The UN General Assembly's Resolution 3314 (XXIX) (Definition of Aggression) is critical because it determines what actions violate sovereignty and further lists seven acts of aggression regardless of a declared state of war. The ICJ acknowledges that this resolution constitutes customary law in its *Nicaragua* judgment. Resolution 3314 states that aggression "is the use of armed force by a State against the sovereignty, territorial integrity, or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[45] Further, Article 3 states that, "any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of Article 2, qualify as an act of aggression:

> (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof,
>
> (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
>
> (c) The blockade of the ports or coasts of a State by the armed forces of another State;
>
> (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
>
> (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
>
> (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;

---

[44] United Nations, *Charter of the United Nations,* Art. 7.

[45] G.A. Res 3314 (XXIX), Definition of Aggression (Dec. 14, 1974), accessed August 21, 2016, http://www.un.org/documents/ga/res/29/ares29.htm

> (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

The provided list of seven acts is not exhaustive and can include additional acts that the UN Security Council deems appropriate, including cyber attacks. An armed response to a cyber attack categorized as an act of aggression can be legally justified; however, use of the term “act of aggression” may not present as strong an argument as “armed attack” would. Cyber acts of aggression also fall under several of these proposed categories. Cyber forces can be considered an attacking force against another nation. Cyber forces have the potential to create a "digital" blockade of goods moving out of port. Cyber forces can directly attack, through digital capabilities, the military of another state. Cyber forces can constitute a type of irregular force conducting an attack with effects similar to a conventional force. The *Nicaragua* judgment supports this claim as it expressly references Article 3, subparagraph (g) of Resolution 3314.[46] The fact that cyber attacks characterized as “acts of aggression” can create effects that previously only traditional military force could accomplish adds weight to the determination that an armed response is legally justified.

The characterization of an action as an “act of violence” also provides legal justification for armed response. The Geneva Conventions and their Additional Protocols I, II, and III are the core of international humanitarian law, the body of international law that regulates the conduct of armed conflict and seeks to limit its effects.[47] Additional Protocol I defines an attack as "violence against the adversary, whether in offense or defense."[48] The United States is not a signatory to

---

[46] Nicar. v. U.S., 1986 l.C.J., 196.

[47] Cornell University of Law, *Geneva Conventions.*

[48] International Committee of the Red Cross, *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, 1125 U.N.T.S. 3.

Protocol I, but does accept many of its provisions as binding customary law.[49] While the term "act of violence" is not as persuasive as "armed attack," a violation of the Geneva Conventions certainly lends credibility to the justification for armed response.

The Council of Europe Convention on Cybercrime of 2001, more commonly known as the "Budapest Convention," requires the signatories to adopt laws against specific activities in cyberspace.[50] Violations of the Budapest Convention may lend legitimacy to an armed response but the violation would have to constitute an armed attack because otherwise action would be limited to only the laws agreed to in the convention such as prosecution in a criminal court. It further requires the cooperation of signatories in the enforcement of the agreed laws. This convention currently has fifty-five signatories of which fifty have now ratified the treaty.[51] (Interestingly, the Philippines, China, and Russia did not sign this convention, causing concern within the United States, as they are the most likely to conduct a cyber attack against the United States). A cyber attack by a private party not acting on behalf of the state in which the private party resides creates a potential dilemma if the offending state refuses to cooperate as required.

A state can be held legally responsible for the criminal actions of a private party, including actions such as cyber attacks. Legal guidelines providing the standard for charging a state for the actions of individuals already exist. In the *Nicaragua* judgment, the ICJ articulated the "effective control standard."[52] In the context of a military operation, a state is responsible for the actions of non-state actors where it is determined that the state has effective control over the

---

[49] Jack M. Beard, "Law and War in the Virtual Era," *American Journal of International Law* 103, no. 3 (July 2009), 426, accessed October 25, 2016. http://www.jstor.org/stable/40283651.

[50] Theohary and Harrington, *Cyber Operations in DOD Policy and Plans*, 23.

[51] Council of Europe, "Chart of Signatures and Ratifications of Treaty 185," *Convention on Cybercrime*, June 12, 2016, accessed January 26, 2017, https://www.coe.int/web/conventions/full-list.

[52] Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 32.

actors in question. The *Nicaragua* judgment does not articulate the measures required to determine this standard.

A possible example of the *Nicaragua* judgment "effective control standard" being applied exists in a case pending litigation at the state level of the United States. In May of 2014, a grand jury in the Western District of Pennsylvania indicted five Chinese military actors for computer hacking, economic espionage, and other offenses directed at six American corporations in the US nuclear power, metals, and solar products industries.[53] US Attorney General Eric Holder stated that this is the first instance of charges of computer hacking brought against another state actor.

Policy and Armed Response

Even if armed response is legally justified, a policy decision must be made about whether it is politically advisable. US cyber policy and the history of armed response to conventional attacks provide additional guidelines to determine how to respond to cyber attacks. Following the policy and history of armed response, several factors for consideration in determining whether an armed response is politically expedient are presented. Hypothetical illustrations of cyber attacks through what-if scenarios outside the norms of conventional attacks can assist government officials to anticipate new threats.

The most recent US cyber policy, President Obama's *International Strategy for Cyberspace*, states that existing law is sufficient for cyber attacks, and acknowledges several aspects of legal justification for an armed response both directly and indirectly. The policy states that a "disruption of networks and systems" could call for a response although it rightfully does

[53] Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," accessed October 25, 2016, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

not state what the response should be. The statement "we fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense."[54] The direct and indirect references for legal justification of an armed response are found in the following excerpt:

> In the case of criminals and other non-state actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend, and prosecute those who intrude or disrupt networks at home or abroad. Internationally, law enforcement organizations must work in concert with one another whenever possible to freeze perishable data vital to ongoing investigations, to work with legislatures and justice ministries to harmonize their approaches, and to promote due process and the rule of law—all key tenets of the Budapest Convention on Cybercrime. When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means, diplomatic, informational, military, and economic, as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests. In so doing, we will exhaust all options before military force whenever we can; will carefully weigh the costs and risks of action against the costs of inaction; and will act in a way that reflects our values and strengthens our legitimacy, seeking broad international support whenever possible.

The obvious reference to the Budapest Convention is noted. A violation of that convention is the least likely scenario to lead to an armed response since other legal methods for response exist. Indirectly, the policy references Article 51 of the UN Charter (right to self-defense), which by itself, can provide justification for armed response.

At a USCYBERCOM[55] Inter-Agency conference in 2012, the US State Department Legal Advisor Harold Koh stated, "Cyber activities that proximately result in death, injury, or

---

[54] President of the United States, *International Strategy for Cyberspace*, 12.

[55] US Army, "U.S. Cyber Command," accessed March 18, 2017, http://www.arcyber.army.mil/Pages/USCyberCommand.aspx. "USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

significant destruction would likely be viewed as a use of force."[56] This is an example of an interchangeable use of terms that could have been better characterized as an "armed attack" rather than "use of force," satisfying the United States and Tallinn Manual definitions of a cyber attack. It is assumed that his use of the term "use of force" refers to an action that has reached the scale and effects threshold to constitute armed attack. Koh further states, "there is no legal requirement that the response to a cyber armed attack take the form of a cyber action, as long as the response meets the requirements of necessity and proportionality." His response is consistent with the LOAC. This conference is the first time the US State Department took a public stance on hostile cyber attacks and the potential of armed response.[57]

Physical attacks and threats to US national interests historically have warranted an armed response. Armed response to a cyber attack is no different than an armed response to a conventional attack in a formal declaration of war or in an AUMF. Congress, by authority of the Constitution of the United States, has the power to declare war.[58]Armed response comes in the form of a declaration of war or the authorized use of military force (AUMF). Armed response for cyber attacks is more likely to occur as an AUMF since formal declarations of war have fallen out of favor.[59] The US Constitution governs the circumstances for a declaration of war, and an AUMF.

To better understand the circumstances under which the United States is likely to mount an armed response to a cyber attack, it is useful to consider the circumstances under which it has

---

[56] Chris Borgen, "Harold Koh on International Law in Cyberspace," Opinio Juris, accessed March 16, 2017, http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/.

[57] Theohary and Harrington, *Cyber Operations in DOD Policy and Plans*, 21.

[58] *The Constitution of the United States*, Article 1, Section 8.

[59] Jennifer K. Elsea and Richard F. Grimmett, *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications* (Washington, DC: Congressional Research Service, 2014), summary, accessed January 15, 2017, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA521125.

mounted an armed response to a conventional attack. Congress approved declarations of war eleven times in five different wars.[60] In these declarations, precipitating acts included a direct attack on the United States, such as the attack on Pearl Harbor in 1941. Attacks on our national interests, such as the German attacks on United States's commercial vessels in 1917, precipitated our entrance into World War I. A cyber attack could also be a direct attack on the United States or its interests, with effects comparable to those of the attack on Pearl Harbor. The drafting of other declarations of war were a response to declarations of war against the United States such as by Italy, Bulgaria, and Rumania during World War II.

Since the period post-WWII, the United States and other countries have refrained from describing conflict and aggression as a state of war.[61] An example of this is the change of language and title from the Law of War to the Law of Armed Conflict. Congress's first use of AUMF was against France in 1798 to protect the US commercial shipping enterprise against French seizure of US vessels.[62] Congress has also authorized the use of military force upwards of 200 times. The United States has conducted armed response for reasons other than an attack on the United States, such as the response to the 1991 invasion of Kuwait.[63]

Just because there is a legal justification for an armed response to a cyber attack, it does not mean that the political situation requires an armed response. However, if a catastrophic cyber attack results in large-scale physical damage and a large death toll, the decision to undertake an armed response appears clear. The more difficult decision is whether an armed response is required to a cyber attack that is not necessarily determined to be catastrophic. The decision involves taking into account a number of interrelated factors to determine if the attacks meets the

[60] Elsea and Grimmett, *Declarations of War and Authorizations for the Use of Military Force*, 1.

[61] Ibid., 21-22.

[62] Ibid., 5.

[63] Ibid., 12-13.

United States scale and effect threshold for an armed response. The United States rightly has not published or stated what the threshold actually is. An armed response should not be taken hastily as it may have negative effects that require careful consideration prior to expending our precious capital and resources. Additionally, consideration of the effects and implications of inaction is important. Combinations of the proposed decision criteria are to be considered on a case-by-case basis every time a decision to undertake armed response that is legally justified is required.

The following list of factors is not exhaustive and can be expanded as required. These factors are linked to the legal justification for armed response and should not be considered separate in analysis. These factors are interrelated, and discussion must transpire in a manner that reflects that idea. Failure to do so, by looking at each factor as if it were independent, may lead to armed response that is not politically advisable.

1. Severity. Perhaps the most important of all factors, this includes scope, duration, intensity, and damage assessment. The physical or logical scope of a cyber attack can be limited or broad, spreading throughout a wider geographic or logically networked region. An example of limited scope is a cyber attack against specific web traffic (rather than denying all traffic) or against a specific device. The scope of a logically dispersed cyber attack could be against an entire command and control system. The duration of a cyber attack and its effects can be for minutes, days, or months. Duration is important more for political concerns because the US population may demand elevated responses, such as armed response, due to lasting effects. Attacks that are short in duration may be forgotten, leading to less demand for armed response. Certain actions can be quite intense but only last a short amount of time. An example might include hacking into Wall Street to make it appear that the market is crashing. The damage assessment for determining severity is critical to events that might not be considered catastrophic. This will lead to a tolerance threshold used on a case-by-case basis and includes consideration of unacceptable loss.

2. Human Casualties. The number of casualties, both wounded and killed, is linked to severity but a separate category altogether due to the intense reaction that results from a loss of life. Some attacks may be limited in duration and intensity and still have a large human toll. There should not be a finite number of deaths or wounded that is considered a static threshold as it would limit options and potentially force commitment of an armed response. An example of why it is important not to have a certain number requirement is if a very high-ranking government official is killed as a result of a cyber attack that triggers a presidential order of succession event. If a specific number existed, it certainly would not be a death or casualty toll of one.

3. Timing of Discovery (Immediacy). The very nature of cyberspace allows effects, to include catastrophic effects, to build slowly over time rather than occur immediately. Timing affects the decision for armed response because political leaders are more likely to consider a cyber attack that has immediate effects to be an armed attack compared to one that builds slowly over time. The link to severity is crucial because the additive effects over time could be considered similar to the effects of a shock that is immediately felt.

The stopping of an event before it occurs that otherwise would have been catastrophic through defensive action is also important because it is linked to the right to self-defense. The method in which the United States stops a cyber attack might create an argument for adversaries to use against the United States that the action was not proportional or was unprovoked. (Attribution of the expected cyber attack is critical.) In this case, the potential for a dangerous cycle of proportional response actions may occur because the argument that "they did it first" materializes.

4. Attribution. Although extremely difficult to determine in cyber attacks, the proof of the attacker's identity is required before an armed response occurs. As the Estonia cyber attack demonstrates, attribution may be the primary factor limiting the legal justification for armed response. Yet, in the cyber domain, proving attribution may also convey information about the

tools that the United States has at its disposal, so divulging that information is politically risky. Getting attribution wrong can lead to an action that is illegitimate and carries a severe consequence of entering armed conflict against a country that is not responsible for the precipitating attack. An example of incorrect attribution is the earlier-mentioned words of Deputy Secretary of Defense John Hamre who stated that he thought that Iraq was responsible for the 1998 "Operation Solar Sunrise" attack on DoD networks, which might have led the United States to enter armed conflict with Iraq mistakenly. Attribution is critical when dealing with non-state actors who may or may not be determined to be under the control of a state according to law.

5. Political Situation. What is the political situation of the United States? Although some may disagree, politicians should weigh the political support for an armed response as they are under the control of the people they represent. Political expedience has and will continue to be a factor for consideration. A president must weigh the consequences of entering armed conflict and the popular support that the American public will provide. Like it or not, the timing of elections will bear on the decision for an armed response. History has demonstrated that armed conflict lacking popular support does not turn out positively for the United States. Examples include the conflicts in Korea, Vietnam, and Iraq.

There are also factors that appear rational, but actually do not matter in determining whether an armed response to cyber attacks is advisable. Some have argued that they are important but for different reasons than this monograph proposes, such as the Tallinn Manual's consideration of "Military Character" which this monograph calls "specificity of target." These factors are not included because they deal primarily with legal justification rather than political consideration or because they are simply not relevant to the discussion.

1. Specificity of target. Military necessity is a principle under the LOAC and the basic premise behind it is that only military objects can be attacked, such as military installations, networks, and formations. In the context of cyber attacks, where civilian targets are just as likely

to be attacked as military targets, it should not matter what the target is because either way, justification for armed response may exist without regard to the nature of the target. Civilian targets may be less defended than military targets thus making them easier to attack. The determination depends on whether the attack reaches the threshold for an armed attack, not what the attack was against. Specificity of target is considered in determining legal justification, and is not a policy factor.

2. Intent. The “I did not mean or intend for that to happen” defense should not be a consideration. Intent as a consideration seems rational, but actually, in the context of cyber attacks, does not matter because as seen in cyber attacks such as Stuxnet, the resulting impact of a cyber action may far exceed the intended impact. This consideration is similar in nature to a collateral damage estimate that is wrong when dropping conventional bombs where the damage of the blast far exceeds the estimate. A proportional armed response may be legally justified for conventional attacks that miss the intended target or a blast that does far greater damage than intended. The intent of a cyber attack that meets the level of an armed attack has no bearing on the decision for armed response and is irrelevant for policy consideration.

It is imperative that the readers of this monograph understand the interconnectedness of these factors. It must be stressed again that government officials cannot and must not focus on individual factors as it may limit their response or force a decision that is not wanted. A factor must not be weighed alone without consideration of how one factor affects or is affected by other factors.

Hypothetical illustrations of cyber attacks through what-if scenarios outside the norms of conventional attacks can assist government officials anticipate new threats. These examples are not to be considered as actual events that have taken place or that are planned to be carried out. The examples assume any level of attacker ranging from individual, group, organization, state, or non-state actor can carry out the attack and so the term "actor" will categorize them all equally

since international courts have held that states can be held responsible for the actions of non-state actors. The first example is the more obvious example that can lead to armed response as it satisfies more of the criteria and is a type of worst-case scenario. The second example is one in which it is harder to determine whether an armed response is justified as it is an "outside the box" scenario.

Attack on government services during a national disaster response action. Imagine an actor that had used a zero-day vulnerability or some form of malware to get into the networked operations that government requires during states of emergency. Following a natural disaster, actors could attack government organizations such as Federal Emergency Management Agency (FEMA) and non-governmental organizations through the digital systems that they use to bring support to the affected area, causing massive delay and chaos. The options could include attacks on systems such as transportation systems used to coordinate logistical supply operations and first responder networks, which provide necessary and immediate critical response to victims of a natural disaster. Either of these could result in unnecessary suffering and potentially death. Looking back at the political environment following Hurricane Katrina in 2005 gives an indication of the kind of confusion and anger an attack of this nature could cause. Certainly, an attack of this sort is unquestionably severe in nature. The duration could last for weeks or months. An attack of this nature potentially violates both the Geneva Conventions and the Hague Conventions, lending legitimacy to an already politically acceptable armed response.

Social Security Administration attack. It is not in the realm of the impossible for an actor to attack the Social Security Administration. This attack would be seen as unconventional in nature and completely devoid of any claim of military necessity. What it could accomplish is the complete destruction of social security information for up to 318 million Americans. The effects that occur following an attack such as this extend to all aspects of our way of life. The negative effects include a stopping of the distribution of social security checks, disruption of military pay

and orders processes, income tax problems, birth and death certificate errors, just to name a few. The list can grow extensively given the pervasiveness of the social security number in the daily lives of Americans. CNN reported that approximately 14,000 Americans are mistakenly entered into Social Security Administration's Death Master File annually.[64] The report explains the negative economic and psychological impact this error has on people. Would the economic impact to "virtually" declaring 318 million people dead be considered catastrophic enough to warrant the use of military force? What if the number were significantly less? This attack may be difficult to categorize as catastrophic because the attack likely would not result in large-scale physical damage or actual death. The intensity of this attack could be quite harsh depending on the effects that occur as a result. The duration of the attack may not have to last very long to have drastic and lasting effects. While the scope of the attack appears limited on its face, focused only on the digital data of the Social Security Administration network, it would have negative effects across the banking industry, the political environment, the military, and the potential for cascading effect in the global market system. An attack such as this meets the two definitions of cyber attack. Legal justification and the political need may exist for an armed response to a cyber attack of this nature.

Conclusion

The potential now exists for catastrophic harm from a cyber attack. The focus on whether cyber attacks are "acts of war" is misplaced and creates a perception that the United States will respond with a declaration of war. Armed response is not limited to declarations of war, which have fallen out of favor, and is more commonly conducted through an authorization of use of military force. Existing international law is sufficient to justify an armed response to a cyber

[64] Blake Ellis, "Social Security Wrongly Declares 14,000 People Dead Each Year," *CNN Money*, August 17, 2011, accessed January 25, 2017, http://money.cnn.com/2011/08/17/pf/social_security_deaths_mistakes/index.htm.

attack. The current cyber policy of the United States supports this claim. Political leaders must have the legal justification for armed response but must also mitigate political risk. Deciding if the political risk is worth the cost of armed response to a cyber attack requires the analysis of certain factors after the armed response is legally justified. Political leaders need to determine the likelihood of attack, and look at the effects of multiple types of scenarios, not just the worst case.

Bibliography

Beard, Jack M. "Law and War in the Virtual Era." *American Journal of International Law* 103, no. 3 (July 2009): 409-445. Accessed October 25, 2016. http://www.jstor.org/stable/40283651.

Borgen, Chris. "Harold Koh on International Law in Cyberspace." Opinio Juris. Accessed March 16, 2017. http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/.

Brangetto, Pascal, Tomas Minárik, and Jan Stinisson. "From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications." *NATO Legal Gazette*, no. 35 (December 2014): 16-28.

Cornell University of Law. *Geneva Conventions*, August 6, 2007. Accessed December 15, 2016. https://www.law.cornell.edu/wex/geneva_conventions.

Cottim, Armando A. "Cybercrime, Cyberterrorism and Jurisdiction. An Analysis of Article 22 of the Coe Convention on Cybercrime." In *Law and Technology: Looking into the Future: Selected Essays.* Edited by Meritxell Fernández-Barrera Norberto Nuno Gomes de Andrade,Primavera De filippi, Mario Viola De Azevedo Cuna, Giovanni Sartor, and Pompeu Casanovas, 69-94. Florence: European Press Academic Publishing, 2009. Accessed December 15, 2016. http://www.ejls.eu/6/78UK.htm.

Council of Europe Convention on Cybercrime. June 12, 2016. 1949, C.E.T.S. 185.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *WIRED*, August 21, 2007. Accessed January 26, 2017. https://www.wired.com/2007/08/ff-estonia/.

Department of Justice. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." Accessed October 25, 2016. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Discover Diplomacy. "What is a U.S. Embassy?" Accessed October 25, 2016. https://diplomacy.state.gov/discoverdiplomacy/diplomacy101/places/170537.htm.

Elsea, Jennifer K., and Richard F. Grimmett. *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications*. Washington, DC: Congressional Research Service, 2006. Accessed January 15, 2017. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA521125.

Goodin, Dan. "How Soviets Used IBM Selectric Keyloggers to Spy on US Diplomats." Ars Technica, October 13, 2015. Accessed August 21, 2016. http://arstechnica.com/security/2015/10/how-soviets-used-ibm-selectric-keyloggers-to-spy-on-us-diplomats/.

Human Rights Library. "Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX)." Accessed October 20, 2016. http://hrlibrary.umn.edu/instree/GAres3314.html.

International and Operational Law Department. *Law of Armed Conflict Deskbook*. Charlottesville, VA: The Judge Advocate General's Legal Center and School, 2012.

International Committee of the Red Cross (ICRC). *IHL and Other Legal Regimes-Jus Ad Bellum and Jus in Bello*. Accessed December 15, 2016. https://www.icrc.org/eng/war-and-

law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm.

———. *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, 1125 U.N.T.S 3.

International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons*. Nuclear Weapons Advisory Opinion, No. 226, July 8, 1996.

———. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Judgment, 1986 I.C.J. Rep. 14, ¶ 191 and 195 (June 27).

———. *Statute of the Court*. Accessed September 22, 2016. http://www.icj-cij.org/documents/?p1=4&p2=2#CHAPTER_II.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon and Schuster, 2016.

Kissel, Richard, ed. NIST IR 7298, no. 3, *Glossary of Key Information Security Terms*. Gaithersburg, MD: National Institute of Standards and Technology, 2013. Accessed February 25, 2017. https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/NIST.IR.7298r2.pdf.

North Atlantic Treaty. April 4, 1949. 63 Stat. 2241. 34 U.N.T.S 243.

NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE). "Cyber Definitions." May 26, 2014. Accessed January 26, 2017. https://www.ccdcoe.org/cyber-definitions.

President of the United States. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: The White House, 2011. Accessed December 15, 2016. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

Sanger, David E. "Obama Ordered Wave of Cyberattacks Against Iran." *The New York Times*, June 1, 2012. Accessed January 26, 2017. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Theohary, Catherine A., and Anne I. Harrington. *Cyber Operations in DOD Policy and Plans: Issues for Congress*. Washington, DC: Congressional Research Service, 2015. Accessed October 25, 2016. https://pdfs.semanticscholar.org/73f1/5e0fb26f8ad007d1f8257651fd04f45691e8.pdf.

U.S. Army. "Cyber Command." Accessed March 18, 2017. http://www.arcyber.army.mil/Pages/USCyberCommand.aspx.

U.S. Congress. House. *Cyber Act of War Act of 2016*, H.R.5220, 114th Cong. (2015-2016). June 7, 2016. Accessed August 21, 2016. https://www.congress.gov/bill/114th-congress/house-bill/5220/actions.

US Congress. Senate. *Cyber Act of War Act of 2016*, S.2905, 114th Cong., 2nd Sess. (2015-2016). Accessed October 25, 2016. https://www.congress.gov/bill/114th-congress/senate-bill/2905/text.

United Nations. *Charter of the United Nations*. Accessed August 21, 2016. http://www.un.org/en/charter-united-nations/.

Yale Law School. "Laws of War: Laws and Customs of War on Land (Hague IV); October 18, 1907." Accessed December 15, 2016. http://avalon.law.yale.edu/20th_century/hague04.asp#art54.

Zenko, Micah. "The Existential Angst of America's Top Generals." *Foreign Policy*, August 4, 2015. Accessed March 1, 2017. https://foreignpolicy.com/2015/08/04/the-existential-angst-of-americas-top-generals-threat-inflation-islamic-state/.