Utah Law Review

Volume 2018 | Number 2 Article 6

5-2018

The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an "Act of War?"

Christopher M. Sanders

THE BATTLEFIELD OF TOMORROW, TODAY: CAN A CYBERATTACK EVER RISE TO AN "ACT OF WAR?"

Christopher M. Sanders*

I. INTRODUCTION

"War. War never changes."[1] Such a phrase has resonated throughout all of human history. Brutal, forceful, evil, murderous, barbaric. War has taken different forms in different domains such as land, air, and sea. From fists to spears; from spears to swords; from swords to all manner of firearms. But now, for the first time in human history, war has changed. No longer are the effects of war felt through the intensity of nuclear warheads, the sound of armed combat, or the booming of cannons. Rather, the effects of war are felt through the whisper heard from the click of a computer. Cyberspace is now the domain of war.[2]

The United States federal government is responsible for defending the American people. "Until recently, the government has fulfilled that role almost exclusively through nuclear deterrence and conventional military forces."[3] But war has changed, and society must adapt to its changes to effectively defend our borders.

Such a statement begs the question: What constitutes an act of war in cyberspace? The developed world has adopted provisions, laws, and agreements dealing with acts of war on land, air, and sea. The leading modern example of military law and alliance is the North Atlantic Treaty Organization ("NATO"). NATO, an alliance between twenty-eight different nations, is one of the longest standing military alliances in recent history.[4] Article V of the North Atlantic Treaty elicits a response from the twenty-eight nations of NATO in response to "armed attacks."[5] This underscores the policy that if you interfere with one, you deal with all. Yet, despite NATO's history and prestige, it remains in its current state unfit to handle acts of terror and war in cyberspace because it has yet to define when such acts occur. Cyberattacks do not precisely fit the criteria of "armed" conflict or an

---

 J.D. candidate at the University of Utah S.J. Quinney College of Law. Executive Text Editor for the *Utah Law Review*. Special thanks to those involved in editing on the *Utah Law Review* and my family for their support and love.

[1] Ron Perlman, FALLOUT 3 (Bethesda Softworks LLC 2008).

[2] *See* Steve Evans, *Cyberspace is New Domain for War: NATO*, INFOSECURITY MAGAZINE (June 16, 2016), http://www.infosecurity-magazine.com/news/cyberspace-is-new-domain-for-war/ [https://perma.cc/2T8K-SCN7].

[3] Mike Rounds, *Defining a Cyber Act of War*, WALL ST. J. (May 8, 2016), http://www.wsj.com/articles/defining-a-cyber-act-of-war-1462738124 [https://perma.cc/UYA4-CLXU].

[4] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243 (signing the Treaty were Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, the United Kingdom, and the United States).

[5] *Id.*

"act of war." Rather, cyberspace remains something misunderstood in its own ethereal and unknown realm.

Cyber warfare is a twenty-first century concept, one that we have only begun to comprehend and develop. Part II develops the science and recent history behind incidents involving cyberspace. Part III argues that cyberattacks can constitute an armed attack or an act of war through triggering the right to self-defense. Part IV proposes a tiered analysis and subsequent response to military incidents involving cyber. Part V recommends modification to the North Atlantic Treaty and similar treaties, laws, and agreements so that they can effectively and efficiently implement these suggestions to respond to what is now considered "21st century warfare." [6] Part VI concludes and summarizes.

II. THE SCIENCE AND RECENT HISTORY OF INCIDENTS INVOLVING CYBER

A. The Creation of the Internet

Everything has a beginning—even cyberspace—which is largely a byproduct of the internet. It is important to understand the origin of cyberspace to more fully comprehend and anticipate its future. Michael Gervais, in his article titled *Cyber Attacks and the Laws of War*, discusses this and the inception of cyber warfare from its initial moorings.[7] He notes that the Cold War acted as a catalyst to the creation of the Internet.[8] The article also notes that "[a]fter World War II, tension quickly escalated between the United States and the Soviet Union. The Soviet Union's launch of the Sputnik satellite in 1957 caused particular alarm in the United States."[9] The United States government began to emphasize technology and science to gain footing in the conflict and created a new agency called the Advanced Research Projects Agency ("ARPA"), which was "invaluable for the creation of the internet."[10]

The ARPA worked to invent a system of communication that would be difficult to detect and intercept by breaking up messages into smaller components spread across different nodes or routes of networking.[11] The most difficult challenge was "figuring out how to make all of the computers work together."[12] Because computers needed to adopt a standard and universal protocol, "Robert Kahn and Vinton Cerf

---

[6] *See* Ty Cobb, *Cyber Warfare: Where the 21st Century Conflicts Will be Fought*, HARV. NAT'L SECURITY J. (Mar. 5, 2012), http://harvardnsj.org/2012/03/cyber-warfare-where-the-21st-century-conflicts-will-be-fought/ [https://perma.cc/VJG7-SE2S].

[7] Michael Gervais, *Cyber Attacks and the Laws of War*, 1 J.L. & CYBER WARFARE 8 (2012).

[8] *Id*. at 11.

[9] *Id*.

[10] Gervais, *supra* note 7, at 12; *see also* Larry Abramson, *Sputnik Left Legacy for U.S. Science Education*, NPR (Sept. 30, 2007), http://www.npr.org/templates/story/story.php?storyId=14829195 [https://perma.cc/N8LR-3P8M].

[11] Gervais, *supra* note 7, at 12.

[12] *Id.* at 15.

designed the standard protocol that is still in place today—the Transmission Control Protocol/Internet Protocol (TCP/IP). [Which] specifies how data should be formatted, addressed, transmitted, routed, and received at the destination."[13] This became the "ARPANET." When the ARPANET adopted TCP/IP in 1983, the Internet was born.[14]

B. The Creation of Cyberattacks

The Internet's creation allowed individuals to traverse this new domain which both fostered and hindered its progression, inevitably leading to the creation of cyberattacks. Cyberattacks occur most often through the accessing of a computer or other electronic system without the owner's consent through Malware.[15] "Malware—similar to software—consists of programs or protocols that tell computers what to do. Those instructions are often destructive, intrusive, or annoying. Unfortunately, just as software has become more innovative and sophisticated over time, so, too, has malware."[16] Malware began with the Creeper Virus, essentially a mere annoyance, which would simply display the message "I'M THE CREEPER: CATCH ME IF YOU CAN."[17] Malware evolved shortly thereafter in 1988 with the Morris Worm, which infected 10% of all computers connected to the Internet.[18] What began as mere annoyance quickly escalated into inflicting harm and destroying property from the inside, which evolved into "cyber-crimes."[19] "It was not long before states began using malware as a method of attacking adversaries in what is now known as a cyberattack."[20]

---

[13] Gervais, *supra* note 7, at 15.

[14] *See* Mitch Waldrop, *DARPA and the Internet Revolution*, DARPA: 50 YEARS OF BRIDGING THE GAP 78, 85 (2008), https://www.darpa.mil/attachments/(2O15)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20Internet%20(Approved).pdf [https://perma.cc/Z8UY-XJAQ].

[15] Gervais, *supra* note 7, at 16.

[16] *Id.* at 16–17.

[17] Georgi Dalakov, *First Computer Virus of Bob Thomas*, HISTORY OF COMPUTERS, http://history-computer.com/Internet/Maturing/Thomas.html [https://perma.cc/MLX6-2V24].

[18] *See* Brian Krebs, *A Short History of Computer Viruses and Attacks*, SECURITY FOCUS (Feb. 14, 2003), http://www.securityfocus.com/news/2445 [https://perma.cc/5S2F-XESG]; Gervais, *supra* note 7, at 17.

[19] Gervais, *supra* note 7, at 17.

[20] *Id.* at 17.

Another form of cyberattack is accomplished with what is known as a botnet. Botnets are defined as "[a] network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam."[21] The impact of botnets has been colossal: the damage caused by botnets is estimated to be greater than "$113 billion in losses globally, with approximately 375 million computers infected each year, equaling more than one million victims per day, translating to 12 victims per second."[22]

C. Recent Incidents in Cyberspace

We live in an electronic world. Society is perpetually surrounded by cyberspace through our phones, computers, cars, televisions, and much more. It takes on even more forms—intangible and ominous—including internet connectivity, satellite transmission, and radio waves. Because of this, the science behind cyberspace is difficult to fathom. The discovery of cyberspace raises questions as to its real origin. For example, NASA occasionally receives unexplained cyber transmissions from deep space.[23] Cyberspace could very well evolve in the future. What is known as cyberspace today may be entirely different in a century, or even a decade from now. Because of the omnipresence of cyberspace in much of the developed world, any form of cyberattack is conceivable. There is no real limit to what "hackers" can do.

Take, for example, a simple automobile. Electric vehicles are becoming increasingly popular. As of the date of this Note, over half a million electric vehicles have been sold in the United States alone.[24] With this rapid increase in electric vehicles also comes the possibility of a cyberattack on such vehicles. Recently, hackers demonstrated that it is possible to "remotely unlock the [Tesla] Model S' doors, start the vehicle and drive away."[25] Hackers can even "issue a 'kill' command to a [Tesla] Model S to shut down the vehicle's systems, bringing it to a stop," all

---

[21] *Botnet*, NEW OXFORD AMERICAN DICTIONARY (3d ed. 2015).

[22] Robert Anderson, Jr., *Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland*, FBI (Sept. 10, 2014), https://www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland [https://perma.cc/2HA4-AEJ3].

[23] *See* Fiona MacDonald, *Mysterious Repeating Radio Signals Have Been Detected Coming From Outside Our Galaxy*, SCI. ALERT (Mar. 3, 2016), http://www.sciencealert.com/mysterious-repeating-radio-signals-have-been-detected-coming-from-outside-our-galaxy [https://perma.cc/PK47-Z2VZ]; Robin Seemangal, *Not a Drill: SETI Is Investigating a Possible Extraterrestrial Signal From Deep Space*, OBSERVER (Aug. 29, 2016), http://observer.com/2016/08/not-a-drill-seti-is-investigating-a-possible-extraterrestrial-signal-from-deep-space/ [https://perma.cc/2AEY-FRQD].

[24] *See* Jeff Cobb, *Americans Buy Their Half-Millionth Plug-in Car*, HYBRID CARS (Sept. 1, 2016), http://www.hybridcars.com/americans-buy-their-half-millionth-plug-in-car/ [https://perma.cc/3SSU-KY2U].

[25] Antuan Goodwin, *Tesla hackers explain how they did it at Defcon*, CNET (Aug. 9, 2015), https://www.cnet.com/roadshow/news/tesla-hackers-explain-how-they-did-it-at-def-con-23/ [https://perma.cc/DPF2-GRJD].

through the vehicle's onboard network.[26] They were also able to remotely "control the radio and touch screen displays and open and close the trunk."[27] However, such control over vehicles is not confined to purely electronic vehicles. Just before these Tesla hackings, cybersecurity researchers were "able to take remote control of a Jeep Cherokee, leading Fiat Chrysler Automobiles to recall 1.4 million vehicles."[28]

Conversely, there are valid arguments that hacking can be used for good instead of evil. Consider a recent conviction of Deric Lostutter who indirectly aided the government in identifying individuals who committed rape in Steubenville, Ohio.[29] In 2012, two males gang-raped a sixteen-year-old female after she passed out from intoxication.[30] The males removed her clothing, penetrated her vagina and forced their penises into her mouth while she was unconscious.[31] Moreover, the males photographed the incident to show their crimes to their friends.[32] A hacker, Deric Lostutter, from "Anonymous"—an underground organization known for its threats and actions in cyberspace—gained access to these photographs through cyberspace and threatened to release them if they did not publicly apologize for their heinous crimes.[33] The rapists were eventually prosecuted and incarcerated for a term of approximately twelve to twenty-four months.[34] The hacker, Deric Lostutter, pled not guilty and was recently sentenced to twenty-four months incarceration—twelve months more than what one of the rapists received—for multiple counts under the Computer Fraud and Abuse Act.[35] Such a disparity among punishments reflects our

---

[26] *Id.*

[27] Samantha Masunaga, *Researchers Hack a Tesla Model S, Bring Car to Stop*, L.A. TIMES (Aug. 6, 2015), http://www.latimes.com/business/la-fi-hy-tesla-hack-20150806-story.html [https://perma.cc/6852-QV6H].

[28] *Id.*

[29] *See* Andrew Blake, *Deric Lostutter, Hacktivist, Charged Over Anonymous Cybercampaign Spurred by Steubenville Rape Cases*, WASH. TIMES (July 7, 2016), http://www.washingtontimes.com/news/2016/jul/7/deric-lostutter-hacktivist-charged-over-anonymous-/ [https://perma.cc/65YY-X7XR].

[30] *See* Richard A. Oppel Jr., *Ohio Teenagers Guilty in Rape That Social Media Brought to Light*, N.Y. TIMES (Mar. 17, 2013), http://www.nytimes.com/2013/03/18/us/teenagers-found-guilty-in-rape-in-steubenville-ohio.html?_r=0 [https://perma.cc/RLG6-H5RQ].

[31] *Id*.

[32] *Id*.

[33] *See* Crimesider Staff, *Hacker Who Called Attention to Ohio Rape Case Facing Charges*, CBS NEWS (July 12, 2016), http://www.cbsnews.com/news/steubenville-ohio-hacker-kyanonymous-who-called-attention-to-rape-case-facing-charges/ [https://perma.cc/7XHD-FB89].

[34] *Id*.

[35] *See* Andrew Blake, *Deric Lostutter, hacker, sentenced to 2 years in prison for crimes tied to Steubenville rape case*, WASH. TIMES (Mar. 8, 2017), http://www.washingtontimes.com/news/2017/mar/8/deric-lostutter-hacker-sentenced-2-years-prison-cr/ [https://perma.cc/8ULY-AFRA]; *see also* Cortney Drakeford, *Deric Lostutter Faces More Prison Time than Football Players*, INTERNATIONAL BUSINESS TIMES (Sept. 8, 2016), http://www.ibtimes.com/steubenville-rape-case-update-hacker-deric-lostutter-faces-more-prison-time-football-2413322 [https://perma.cc/359B-5EYC].

cultural fear of cyberspace: a fear of the unknown. We fear the apparent unlimited power of a cyberattack.

Some of the more popular episodes involving cyberspace include the hack into the Democratic National Committee and AshleyMadison.com. Ashley Madison is a website directed towards males and females who are married but still wish to date.[36] Its slogan was "Life is short. Have an affair."[37] Participation on Ashley Madison requires creating a personal account and profile.[38] The information was apparently kept confidential and discreet.[39] Prior to this incident, customers could also pay an additional fee to have that information deleted in "cyberspace."[40] In 2015, the website garnered national attention after hackers stole and released the customers' information.[41] The release included emails, names, home addresses, sexual fantasies, and credit card information shown in the customers' profiles.[42] The hack affected over thirty million customers.[43] The hackers threatened to release the information if the site was not closed by a specific date.[44] Because the website was still up by the threatened date, true to their word, the hackers released all of the information—including the information of those customers that paid an extra $19 fee to have their data "deleted."[45] The consequences were severe: suicide, multiple class action lawsuits seeking in total over $1 billion in damages, six-figure bounty offers for finding the hacker, job loss, and much more.[46]

---

[36] ASHLEY MADISON, https://www.ashleymadison.com/?reg=1 [https://perma.cc/72P9-XJNV].

[37] *Id.*

[38] Frequently Asked Questions, ASHLEY MADISON, https://www.ashleymadison.com/app/public/faq.p [https://perma.cc/6YTL-BMR2].

[39] *Id.*

[40] *See* Team Register, *What Ashley Madison Did and Did NOT Delete If You Paid $19–and Why It May Cost It $5m+*, THE REGISTER (Aug. 25, 2015), http://www.theregister.co.uk/2015/08/25/us_class_action_ashley_madison/ [https://perma.cc/2F5V-5WTD].

[41] *See* Charles Riley, *Hackers Threaten to Release Names from Adultery Website*, CNN MONEY (July 20, 2015), http://money.cnn.com/2015/07/20/technology/ashley-madison-hack/ [https://perma.cc/DH6Y-RV7R].

[42] *Id.*

[43] Melissa J. Sachs, *Cheating Website Ashley Madison Hit with Data Breach Suits*, 33 WESTLAW J. COMPUTER AND INTERNET 6, Sept. 11, 2015, at 1.

[44] *Id.*

[45] *Id.*

[46] Dieter Holger, *8 Consequences of the Ashley Madison Hack*, INQUISITR (Aug. 27, 2015), http://www.inquisitr.com/2366085/8-consequences-of-the-ashley-madison-hack/ [https://perma.cc/URC7-LF7L].

The Democratic National Committee ("DNC")—the governing body of the Democratic party in the United States of America—was also hacked, presumably by Russia, releasing email correspondence between members of the DNC.[47] As a body, the DNC is to remain unbiased towards a specific individual within the democratic party. However, the correspondence released hinted towards the opposite:

> Many of the most damaging emails suggest the committee was actively trying to undermine Bernie Sanders's presidential campaign. . . . [T]hese examples came late in the primary—after Hillary Clinton was clearly headed for victory—but they belie the [DNC's] stated neutrality in the race even at that late stage.[48]

Cyberattacks have also been launched in the last decade against Georgia in its war with the Russian Federation in 2008, against Estonia in 2007, and against the Iranian Nuclear Facilities with the Stuxnet worm in 2010.[49] The Stuxnet worm was designed to attack industrial control systems by forcing "Iran's centrifuges to spin out of control" and to "deceive operators into thinking the machines were operating normally when they were actually tearing themselves apart."[50] The Stuxnet worm affected the entire world, but its harmful effect was directed towards Iran's nuclear program.[51] Iran did not release specific details describing the effects of the attack, but "it is currently estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges."[52]

D. In Response

In response to these ever increasing cyberattacks, the Federal Bureau of Investigation created a Cyber division in 2002. In 2014, the FBI announced the indictments of high profile hackers that had penetrated corporations and stolen millions of dollars and created sophisticated malware—some of which have infected

---

[47] *See* David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. TIMES (Oct. 7, 2016), http://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html [https://perma.cc/Y4N7-YWT5].

[48] Aaron Blake, *Here are the latest, most damaging things in the DNC's leaked emails*, WASH. POST (July 25, 2016), https://www.washingtonpost.com/news/the-fix/wp/2016/07/24/here-are-the-latest-most-damaging-things-in-the-dncs-leaked-emails/ [https://perma.cc/6LXU-DRCA].

[49] INT'L GRP. OF EXPERTS, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 1–2 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

[50] Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L. L. 525, 570 (2012).

[51] *Id.*

[52] Michael Holloway, *Stuxnet Worm Attack on Iranian Nuclear Facilities*, STANFORD U. (July 16, 2015), http://large.stanford.edu/courses/2015/ph241/holloway1/ [https://perma.cc/8U9U-F5AT].

over half a million computers worldwide and stolen more than $100 million in total.[53] "[In August 2014], a federal grand jury indicted Su Bin, a Chinese national, on five felony offenses stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company, which manufactures the C-17 military transport aircraft."[54]

Events such as these have raised eyebrows universally and have earned our worldwide attention and concern. The United Kingdom, in its 2010 *National Security Strategy*, labeled "cyber attack[s], including by other States, and by organised [sic] crime and terrorists" as a "Tier One" threat to their national security.[55] The United States has responded to this new domain of war by creating a new division in its military called "Cyber Command" to effectively respond and potentially attack its enemies in cyberspace. Its mission statement is as follows: "United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries."[56]

NATO also recognized the threat of cyberattacks, committing itself to "develop further [its] ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defen[s]e capabilities . . . and better integrating NATO cyber awareness, warning and response with member nations."[57]

While the world has recognized the threat of cyberattacks and exploitation in cyberspace, it has done little to develop the law surrounding this issue. No one has yet defined when a cyberattack constitutes an act of war.[58] Without a definition or guide to further our understanding, it will remain something misunderstood and feared; and without a clear, universal understanding of cyber warfare, especially in the legal realm, we will remain unprepared to respond to it. Thus, it is necessary to consider when an action is an "act of war" in cyberspace to gain insight into this new domain of war.

---

[53] Robert Anderson, Jr., *Cyber Security, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland*, FBI (Sept. 10, 2014), https://www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland [https://perma.cc/2HA4-AEJ3].

[54] *Id.*

[55] HER MAJESTY'S GOVERNMENT, A STRONG BRITAIN IN AN AGE OF UNCERTAINTY: THE NATIONAL SECURITY STRATEGY 11 (Oct. 2010).

[56] *Our Mission*, U.S. ARMY CYBER COMMAND, http://www.arcyber.army.mil/Pages/ArcyberHome.aspx [https://perma.cc/CBR9-QP8Y].

[57] NATO, ACTIVE ENGAGEMENT, MODERN DEFENSE: STRATEGIC CONCEPT FOR THE DEFENSE AND SECURITY OF THE MEMBERS OF THE NORTH ATLANTIC TREATY ORGANIZATION 16–17 (2010).

[58] *See* Bryant Jordan, *US Still Has No Definition for Cyber Act of War*, MILITARY.COM (June 22, 2016), http://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html [https://perma.cc/RRG8-4YQV].

III. AN ACT OF WAR

An act of war has not been defined in cyberspace. America, and the developed world, need to define and determine exactly when an act in cyberspace can constitute an act of war. Desiree Gargona argues that an act of war is a term of art borrowed from international law.[59] There, it is defined as a "'use of force or other action by one state against another' which '[t]he state acted against recognizes . . . as an act of war, either by use of retaliatory force or a declaration of war.'"[60] Of course, this does little to help a nation who has yet to define "act of war" since the definition presumes the victim state has a definition in place by its own terms. In America, an "act of war" on traditional domains of war is codified and defined in 18 U.S.C. § 2331 as "any act occurring in the course of—(A) declared war; (B) armed conflict, whether or not war has been declared, between two or more nations; or (C) armed conflict between military forces of any origin."[61] However, cyberspace does not involve "arms," leaving a persistent confusion as to what could constitute an act of war in cyberspace.

We have at least one American example of an act of war in recent history, albeit not in cyberspace: September 11, 2001 ("9/11"). On that date, Islamic Extremists hijacked four planes flying above the United States.[62] One of the airplanes flew directly into the north tower of New York's World Trade Center.[63] Minutes later, a second plane flew into the south tower.[64] A third plane flew into the Pentagon, with a fourth crashing in a field in Shanksville, Pennsylvania.[65] Thousands of Americans lost their lives.[66] The event was indeed an act of war that triggered the right of self-defense for the American people.[67] However, some scholars disagree over whether 9/11 was, in fact, an act of war.[68] If 9/11 could not reach the threshold of an act of

---

[59] Desiree Gargano, *An Act of War: Finding A Meaning for What Congress Has Left Undefined*, 29 TOURO L. REV. 147, 152 (2012).

[60] *Id.* (quoting JAMES R. FOX, DICTIONARY OF INTERNATIONAL AND COMPARATIVE LAW 6 (1992)).

[61] 18 U.S.C. § 2331(4) (effective Oct. 26, 2001).

[62] *See A Minute-By-Minute Breakdown Of What Happened On 9/11*, HUFFINGTON POST (Sept. 11, 2016), http://www.huffingtonpost.com/entry/9-11-timeline_us_57d300d8e4b06a74c9f48c09 [https://perma.cc/77SL-A29S].

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] Gervais, *supra* note 7, at 37.

[68] *Compare* Michael S. Rozeff, *9/11 Was Not An Act of War*, LEWROCKWELL.COM (Apr. 9, 2015), https://www.lewrockwell.com/2015/04/michael-s-rozeff/911-was-not-an-act-of-war/ [https://perma.cc/A49R-H73H] (arguing that 9/11 was not an act of war because it was not committed by another country or military force), *with* John Siniff, *Voices: By any definition, 9/11 was an 'act of war*,' USA TODAY (Sept. 11, 2014), http://www.usatoday.com/story/news/nation/2014/09/10/voices-911-act-of-war/15385439/ [https://perma.cc/A6RH-LR78] (stating that President Bush and 86% of Americans believed

war thus triggering self-defense, it is nearly unfathomable to ascertain the degree of harm required to reach that threshold as nearly 3,000 innocent people lost their lives that day.

While acts of war are more easily understood on traditional domains of war, such as land, air, and sea, they remain perplexing in their own right. Thus, it is easier to analyze this issue as whether a showing of force triggers the right to national self-defense rather than quibbling over whether an action is an act of war. In this light, it makes sense to analyze "act of war" and "self-defense" synonymously rather than simply blanket labeling heinous uses of force an act of war. Acts of war do not necessarily trigger war in the United States, but rather provide justification to declare war. It is logical, then, to argue that when an action triggers the right to self-defense, then that action would likely constitute an act of war as well. Whenever the term "act of war" is used, it is easier to understand this through analyzing when the right to responsive self-defense is activated.

The NATO Cooperative Cyber Defence Centre of Excellence ("NATO CCD COE") enlisted the help of various international experts to demystify the legal issues of cyberspace in 2009.[69] The result was one of the leading legal documents on issues in cyberspace: the *Tallinn Manual*. It is "[t]he product of a three-year project by twenty renowned international law scholars and practitioners," which discusses the international law applicable to cyber warfare.[70] Through its research and analysis, the *Tallinn Manual* established ninety-five black letter rules governing issues related to cyber conflicts such as "sovereignty, State responsibility, the *jus ad bellum*, international humanitarian law, and the law of neutrality."[71] Following each rule is extensive commentary which explains how each of the experts agreed, or disagreed, on the formulation of each rule.[72] Despite the document's prestige, none of the ninety-five rules directly elaborates on when cyberattacks could amount to war, but rather dictates civility and rules in cyber warfare.[73]

---

that 9/11 was an "act of war"), *with* Brad Reid, *9/11 An 'Act of War' Under Federal Environmental Law*, HUFFINGTON POST (July 27, 2014), http://www.huffingtonpost.com/brad-reid/911-an-act-of-war-under-f_b_5399442.html [https://perma.cc/RNS9-JRKG] (describing a Second Circuit decision holding that 9/11 was an act of war under CERCLA), *with* David T. Ratcliffe, *The 9-11 Bombings Are Not Acts of War, The 9-11 Bombings Are Crimes Against Humanity*, RATICAL.ORG (May 2003), https://ratical.org/ratville/CAH/intro2cah.html [https://perma.cc/LSY5-BDR7] (arguing that the attacks on 9/11 were crimes against humanity, not an act of war).

[69] TALLINN MANUAL, *supra* note 49, at 1 n.1 ("The NATO CCD COE is neither part of NATO's command or force structure, nor funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.").

[70] *Id.* at i.

[71] *Id.*

[72] *Id.*

[73] *See id.*

A. Cyberattacks Can Constitute an Act of War Through Triggering the Right to Self-Defense

The reason such difficulty arises in labeling cyberattacks as an act of war is its inherent nature. It is not exactly "armed" conflict nor always a display of "force." It can be subtle, quiet, unassuming, intangible, and even delayed. Indeed, soldiers would feel more emotionally detached from their actions by design when controlling predator drones than those who face their enemies without an electronic screen between them. Without apparent brutality, an act of war becomes more difficult to define. Moreover, the Department of Defense has yet to define when a cyberattack constitutes an act of war.[74] The line is sharper when labeling acts of war in traditional domains rather than cyberspace. Certain acts are more readily definable as an act of war in land, air, and sea because they either involve armed conflict or they do not, such as 9/11 or the Cuban Missile Crisis. Such attacks are more readily labeled acts of war because "[you] know it when you see it[:]" death and destruction.[75] Cyber warfare, on the other hand, can be much subtler, and much more prolonged or delayed.

Michael Gervais identifies what makes that delineation blurry in cyberspace. He clarifies that some incidents in cyberspace are merely exploitation, rather than attack.[76] For example, the incidents involving Russia and the DNC as well as AshleyMadison.com would likely be exploitation rather than attack. Those incidents were not intended to destroy or cause loss of life, but were rather merely for use in a selfish manner, which fits the definition of "exploitation."[77] But should there be a distinction at all between cyber and traditional domains of warfare? This Note suggests that all domains of war should be analyzed and defined identically, whether they are tangible or intangible.

The primary question is whether cyberattacks can ever qualify as an act of war or reach the threshold of an "armed attack." If the answer is no, then little needs to be done. However, if the answer is yes—as this Note argues—then thresholds must be defined as cyberattacks varying in kind as well as in degree. Indeed, "the Obama administration and the Pentagon made clear that acts like shutting down a U.S. power grid via a cyberattack could indeed qualify as an act of war that would not only bring a similar cyber response but maybe even 'a missile down one of your smokestacks.'"[78]

The 114th session of Congress introduced a bill called the Cyber Act of War Act, directing the President to do two things. First, to "develop a policy for

---

[74] Gervais, *supra* note 7, at 20.

[75] *See* Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (clarifying that obscenity can take an "I know it when I see it" standard).

[76] Gervais, *supra* note 7, at 19.

[77] *See Exploitation*, NEW OXFORD AMERICAN DICTIONARY (3d ed. 2015).

[78] USA Features Media, *When do we call a cyber attack an act of war? No one knows at the moment*, GLITCH NEWS (June 29, 2016), http://www.glitch.news/2016-06-29-when-do-we-call-a-cyber-attack-an-act-of-war-no-one-knows-at-the-moment.html [https://perma.cc/V5DL-BEXS].

determining when an action carried out in cyberspace constitutes a use of force against the United States;" and second, to "revise the Department of Defense Law of War Manual accordingly."[79] In developing the policy behind this law, Congress asks the President to consider "(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[] [and] (2) [i]ntangible effects of significant scope, intensity, or duration."[80] Thus, Congress also agreed that a cyberattack can constitute an act of war, but failed to provide reasonable guidance on how that might be defined.

The two more relevant provisions in the United Nations Charter on this issue are articles 2(4) and 51. Article 2(4) states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[81] This article is primarily known as the use of force article, and by its terms is prohibitory in purpose. The second is article 51, which states "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defen[s]e if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."[82] This provision is also prohibitory in nature, but is even more reactive and entitles a state to respond if unlawful force is used against them. Such a provision would include NATO, as it is a collective provision on self-defense.[83] However, NATO—or any other nation or organization—cannot effectively respond to defend a nation if they have not labeled and defined the threshold of attack that would entitle them to do so.

The reason cyberattacks can qualify, at the very least, as an armed attack is because any weapon can be used to constitute an unlawful use of force.[84] The International Court of Justice ("ICJ"), as the principal judicial organ of the United Nations, noted this by referring to articles 2(4) and 51, stating that "[t]hese provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed."[85]

This notion that anything can be considered a weapon was solidified when, "[t]he Security Council reaffirmed this sentiment when it authorized the United States to respond forcefully in self-defense to the 9/11 attacks, where the 'weapons' were hijacked airplanes."[86] Therefore, "the mere fact that a computer (rather than a more traditional weapon . . .) is used during an operation has no bearing on whether

---

[79] H.R. 5220, 114th Cong. (2d Sess. 2016).

[80] *Id.*

[81] U.N. Charter art. 2, ¶ 4.

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

[83] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246.

[84] Gervais, *supra* note 7, at 37.

[85] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (Jul. 8, 1996).

[86] Gervais, *supra* note 7, at 37.

that operation amounts to a 'use of force.'"[87] That logic leads to the conclusion that the weapon used has no bearing on whether a nation may respond in self-defense per the articles cited in the U.N. Charter. Thus, cyberattacks can invoke the right to self-defense under articles 2(4) and 51 of the U.N. Charter.

B. When Does a Cyber Attack Constitute an Act of War?

The threshold question that must be decided is when a cyberattack rises to an act of war or the right to respond in self-defense, either collectively or individually. One definition might be that any use of force, even in cyberspace, constitutes a *per se* armed attack and thus triggers the right to self-defense.[88] Under this view "any offensive action by a military cyber unit is an armed attack because it emanates from the armed forces of a state."[89] Because this definition is sensitive and malleable, "[t]he danger is that a single errant soldier could embroil a nation in a protracted conflict if his or her action permits the target state to respond in self-defense."[90] This approach appears unreasonable and overbroad as it reaches circumstances that were never intended to be an unlawful showing of force as shown in the example above.

A second, more reasonable possibility is the "scale and effects" test employed by the ICJ.[91] The ICJ finds a real, substantive distinction between an "armed attack" and mere "use of force."[92] To distinguish between the two, the ICJ analyzes the scale and the effects of the attack.[93] By design, not every action by a state in cyberspace triggers the right to collective or individual self-defense because not all presentations of force rise to the level of "armed attack." "To know whether a cyber attack meets the threshold of 'armed attack' requires knowing where the de minimis threshold lies. However, this is a vague and fact-specific rule."[94]

Under the scale and effects test, a cyberattack which inflicts "substantial destruction upon important elements of the target state" through, for example, destruction of property or the loss of lives, would trigger the right to self-defense

---

[87] TALLINN MANUAL, *supra* note 49, at 42.

[88] Gervais, *supra* note 7, at 35–36; *see also* Elizabeth Wilmhurst, *Principles of International Law on the Use of Force by States in Self-Defence* 18 (Chatham House Int'l Law Working Paper, Oct. 2005), http://www.chathamhouse.org.uk/files/3278_ilpforce.doc [https://perma.cc/H3G3-GVAQ].

[89] Gervais, *supra* note 7, at 36.

[90] *Id.*; *see also* Case Concerning Armed Activities on the Territory of the Congo (Dem. Rep. of the Congo v. Uganda), Judgement, I.C.J. 242 (Dec. 19, 2005) ("According to a well-established rule of a customary nature, as reflected in Article 3 of the Fourth Hague Convention respecting the Laws and Customs of War on Land of 1907 as well as in Article 91 of Protocol I additional to the Geneva Conventions of 1949, a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces.").

[91] Gervais, *supra* note 7, at 36.

[92] *Id.*

[93] *Id.*

[94] *Id.* at 36–37.

under article 51.[95] This is also reflected in the *Tallinn Manual* rule 13: "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right to self-defen[s]e. Whether a cyber operation constitutes an armed attack depends on its scale and effects."[96] Despite the division among the experts in the *Tallinn Manual* on many points, the experts agree that as of 2012, no international cyber incidents reached the threshold of an armed attack, and unanimously conclude that a cyberattack, if sufficiently grave, could reach the threshold of an armed attack to trigger a response from a state.[97] In reaching this conclusion, the experts note that biological, radiological, and chemical attacks could constitute armed attack despite the absence of "arms"; thus, cyberattacks could as well.[98]

C. A Modified Scale and Effects Test

The problem with a scale and effects approach lies in timing. By its definition, the scale and effects test requires a state to analyze the *outcome* of an attack to determine its severity. Thus, there can be no real prevention of cyberattacks before they occur if the right to exercise self-defense can only be triggered by the outcome of an unlawful action by another state under this test. It leaves no room for a state to analyze the intended purpose of an impending attack in cyberspace. Rather, it requires a state to sit still and watch. Therefore, the best approach would be a modified scale and effects test, where, if an attack was sufficiently grave and verified to occur, then self-defense would be triggered.

This, in turn, "has led states to turn to customary international law for the determination of when it is appropriate to forestall an attack."[99] The *Caroline* test—whose name is derived from the American Steamboat *Caroline* involved in international disputes between Canada, America, and Britain in the nineteenth century—determines whether a state may take action in anticipatory self-defense.[100]

---

[95] *Id.* at 37.

[96] TALLINN MANUAL, *supra* note 49, at 54.

[97] *Id.* at 54–55.

[98] *Id.*

[99] Gervais, *supra* note 7, at 38.

[100]

> The inherent right to self-defense was first enunciated in the Caroline incident. In 1837, a secret British military unit entered the United States and destroyed the American vessel Caroline, which had been aiding Canadian insurgents fighting against British rule. The incident resulted in the loss of the vessel as well as two American lives. Confronted by American officials, the British maintained that the attack on the Caroline was an act of self-defense. Daniel Webster, the US Secretary of State, wrote a letter in return, demanding that the British justify this claim by showing that the need for self-defense was instant, overwhelming, leaving no choice of means, and no moment for deliberation . . . even supposing the necessity of the moment authorized them to enter the territories of the United States at all, did nothing unreasonable or excessive; since the act, justified by the necessity of self-defence, must be limited by that necessity, and kept clearly

To act in anticipatory self-defense, a state must show "that the 'necessity of self-defense was instant, overwhelming, leaving no choice of means, and no moment of deliberation.'"[101] However, even if these difficult thresholds are met, the response must not be "unreasonable or excessive; since the act, justified by the necessity of self-defense, must be limited by that necessity, and be kept clearly within it."[102]

Concluding that cyberattacks could constitute an armed attack or an act of war leaves open the question of where the *de minimis* threshold lies. Michael Gervais uses two examples to illustrate this point. First, under customary practice, he suggests "that under conventional notions of force, even small-scale bombings, artillery, naval or aerial attacks qualify as 'armed attacks' activating Article 51, as long as they result in, or are capable of resulting in, destruction of property or loss of lives."[103] On the other hand, an action similar to "the firing of a single missile into some unpopulated wilderness as a mere display of force would likely not be sufficient to trigger Article 51, despite violating Article 2(4)."[104]

Through these examples, the *Tallinn Manual* establishes a reasonable definition and answer to cyberattacks in rule 30, which defines cyberattack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[105] The experts argue that this rule should be interpreted broadly.[106] For example, even if the attack is intercepted and caused no damage or injury, it could still rise to the level of a cyberattack because, under this definition, the cyber operation must only be reasonably expected to cause damage to constitute a cyberattack.[107] Moreover, if the actor did not intend the results that followed, it could still constitute a cyberattack if it resulted in substantial destruction of property or loss of life.[108] On the other hand, "[a] cyber attack that merely creates an inconvenience might be a prohibited use of force, but it would not rise to the level of an armed attack. In comparison, a cyber attack capable of substantially destroying property or causing the loss of lives should trigger the right to self-defense."[109]

> within it. The British accepted this test by justifying its actions accordingly. As has been explained by international scholars, the Caroline test requires that nations show that use of force is necessary due to an imminent threat, and that the response is proportionate to the threat.

Adam P. Tait, *The Legal War: A Justification for Military Action in Iraq*, 9 GONZ. J. INT'L L. 96, 111 (2005) (citations omitted).

[101] Gervais, *supra* note 7, at 39 (citing R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AM. J. INT'L. L. 82, 89 (1938)).

[102] *Id.* (citing R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AM. J. INT'L. L. 82, 89 (1938)).

[103] *Id.* at 37 (citation omitted).

[104] *Id.* at 37–38.

[105] TALLINN MANUAL, *supra* note 49, at 106.

[106] *Id.* at 106–10.

[107] *Id.* at 110.

[108] *Id.* at 109.

[109] Gervais, *supra* note 7, at 38.

D. Dealing with Issues in Degree

Another issue with cyberspace and cyberattacks lies in degree. Is there a middle ground between inconvenience or annoyance and destruction of property or the loss of lives? What if the cyberattack merely disables a crucial military defense? Or releases private and personal information about governments or its officials? Should the right to self-defense be triggered then? Perhaps a more appropriate response in these situations would be a mere countermeasure to quell or deter the threat. Rule 9 in the *Tallinn Manual* presents a sound response to such a situation. It states: "A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State."[110] This suggests a countermeasure that would be both similar in degree and kind. Countermeasure, in this context, is a legal term of art and is distinguishable from the military's definition, where countermeasures are more aggressive and seek to destroy rather than merely quell or deter through proportionate response.[111] The experts in the *Tallinn Manual* elaborate on appropriate countermeasures in cyberspace:

> Such countermeasures must be intended to induce compliance with international law by the offending State. For example, suppose State B launches a cyber operation against an electrical generating facility at a dam in State A in order to coerce A into increasing the flow of water into a river running through the two States. State A may lawfully respond with proportionate countermeasures, such as cyber operations against State B's irrigation control system.[112]

After concluding that cyberattacks could rise to an act of war, and that there are questions of degree of harm among other issues, how does one effectively codify the appropriate label and response for each type of attack?

IV. PROPOSING A TIERED ANALYSIS

The only reason cyberspace is so perplexing and complicated in the legal arena is because it is new. The legal realm dislikes new problems because lawmaking draws so much on experience, tradition, and history as a guide to enact, amend or decide a legal issue. Laws take time, experience, and argumentation before much of anything can be accomplished. Among the many statues carved into the United States Supreme Courthouse of the great lawgivers—Moses, Plato, and Confucius—

---

[110] TALLINN MANUAL, *supra* note 49, at 36.
[111] *See id.*
[112] *Id.* at 36–37.

there is also a tortoise.[113] It is a representation of the slow and steady pace the law takes to reach its goal.[114] But rest assured, it reaches the goal. Does the law need to delineate between cyberspace and the more traditional domains of warfare such as land, air, and sea? This Note argues in the negative. Cyberattacks do not need to be separated and treated differently from other acts of war, and such actions in cyberspace should be analyzed identically to the traditional domains of war.

Cyberattacks, despite their realm being intangible, always result—or are intended to result—in a tangible consequence. And that standard should be the base point for determining whether an action constitutes an act of war and where an attack fits into this tiered analysis. The scale and effects test comes closest to this label, notwithstanding the timing issues discussed above. The only question that remains is: What is the result, or intended result, of the cyberattack? We need not fear the realm of cyber, despite what is shown in Deric Lostutter's case.[115] Cyber is merely a route to accomplish indirectly what would be more complicated or dangerous to do so directly. So, why do we treat acts in cyberspace as something more sinister, or more heinous than crimes that are committed directly? The results are the same.

Because cyberattacks can take an infinite number of forms with an infinite variety of results, they should be labeled and analyzed under a tiered structure in order to respond effectively, proportionally, and legally, rather than under the black and white analysis typically taken in traditional domains of war. This Note suggests that a three-tiered approach should be adopted and potential cyberattacks should be labeled to respond effectively and proportionally to those attacks. This specific approach is not about precaution or prevention—which are important goals—but rather, response.

Tier one, the first and highest tier, analyzes the effects of a cyberattack and whether the attack resulted, or was intended to result, in significant destruction of property or the loss of lives. Take, for example, the 9/11 attacks. The United States responded in self-defense against the attacks by Islamic extremists.[116] If the attacks occurred through an electronic hijacking rather than direct hijacking, it is arguable the results would have been the same. Therefore, the United States would still have been free to respond in self-defense in any domain they wished: cyber, land, air, or sea. A cyberattack that would satisfy the tier one threshold would not be confined to a proportionate response in cyberspace. Such a state would be free to choose to respond in self-defense in any way they, and international law, deemed reasonable. Such a response to a tier one cyberattack would not require permission from any agency, committee, or organization, as was the case with 9/11. The response would be immediate and necessary because of its magnitude and severity. Unfortunately, because lawmakers currently quibble over defining an act of war in cyberspace rather than looking to the scale and effects of cyberattacks on states, there remains

---

[113] *See The East Pediment Information Sheet*, SUPREME COURT (May 22, 2003), https://www.supremecourt.gov/about/eastpediment.pdf [https://perma.cc/N52S-LWN3].

[114] *Id.*

[115] *See* Blake, *supra* note 29.

[116] Gervais, *supra* note 7, at 37.

nothing but speculative countermeasures to be implemented by a victim state. This tier also coincides with the *Caroline* test discussed above for anticipatory self-defense.[117]

Tier two, the second highest tier, would be similar to a tier one attack. However, if the cyberattack did not result in the loss of life or significant destruction of property but merely impairment or temporary interference with a nation's critical defenses, infrastructure, or resources, the initial attack would be referred to an international committee, such as the UN, the ICJ, or some newly enacted international organization that can efficiently and competently answer the question of cyber issues and self-defense. For example, NATO must determine for itself that an armed attack occurred to trigger the collective or individual self-defense provision in article V of the treaty.[118] The response, if permitted, would resemble the response triggered in a tier one attack: any action necessary to quell the initial threat. The only difference would be timing. An example of a tier two attack might be an impairment in military defenses, or national satellites that are so crucial to a nation's resources and defenses.

Tier three, the third and lowest tier, would more closely resemble cyber exploitation as it is defined above.[119] Such an attack does not result in significant destruction of property or the loss of lives, nor is it intended to. It is intended to fracture or weaken a government's infrastructure, or even society at large, which is unacceptable. Like a tier two attack, the initial attack would be referred to an international committee, such as the UN, the ICJ, or some newly enacted international organization that can efficiently and competently answer the question of cyber issues and self-defense to provide guidance on further action.

In most circumstances, if the source of an attack could be identified, a proportionate countermeasure would be the most effective response as that term is defined above. The countermeasure would act as both a punitive measure against a state and as a deterrent effect to other nations. Additionally, it would be reflective in both kind and degree to the initial attack. The example used above was an attack on a state's electrical generating facility at a dam to control the flow of water.[120] The appropriate countermeasure, under this tier, would be reflective of the first attack, "such as cyber operations against [the offending state's] irrigation control system."[121] This position is reflective of rule 14 established in the *Tallinn Manual*, which reads "[a] use of force involving cyber operations undertaken by a State in the exercise of its right of self-defen[s]e must be necessary and proportionate."[122]

Such a response is not without its flaws. A proportionate countermeasure against an offending state may not have the same impact as it did on the victim state because injury is relative. For example, if the offending state is a less-developed

---

[117] *See supra* note 100 and accompanying text.
[118] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.
[119] *See supra* note 77 and accompanying text.
[120] TALLINN MANUAL, *supra* note 49, at 36–37.
[121] *Id.* at 37.
[122] *Id.* at 61.

nation as compared to the victim state, then the harm caused by a responsive cyberattack would not be as deleterious. Moreover, it would be more difficult to identify attacks by organizations without tangible boundaries by design—such as ISIS—in cyberspace. Essentially, more developed nations have more to lose. This, in turn, reduces the deterrent effect that underlies the policy behind a countermeasure. However, less-developed nations would be less inclined to execute a sophisticated attack in cyberspace merely because of resources and capability. Despite this somewhat paradoxical effect, lines must be drawn somewhere, and the response argued in a tier three attack appears to be the most reasonable and appropriate response considering the world as a whole.

V. RECOMMENDED MODIFICATIONS TO THE NORTH ATLANTIC TREATY AND SIMILAR TREATIES AND INTERNATIONAL AGREEMENTS

This Note demonstrates the prevalence of cyber issues. These issues will only increase and escalate as time and technology progresses. It may even reach a point where wars are substantially—or even exclusively—fought in cyberspace. Despite the worldwide fear of cyberspace and our attempts to thwart cybercrime, cyberattacks, and cyber exploitation, "there are no treaty provisions that directly deal with 'cyber warfare.'"[123]

One of the leading military alliances and treaties today is the North Atlantic Treaty. "The North Atlantic Treaty Organization was created in 1949 by the United States, Canada, and several Western European nations to provide collective security against the Soviet Union."[124] Despite NATO's prestige and prevalence, its treaty has not yet developed responses to cyberattacks. Nor has most of the modern world in any treaty, nor in any international or domestic law. It is therefore imperative that our laws change with society and technology. It is not acceptable to await devastating attacks in cyberspace before we enact modifications to our existing laws. We must prepare ourselves now. That first requires evolving treaties and laws to reflect the evolution occurring in warfare. Thus, to the extent possible, states and organizations such as NATO, should take appropriate steps to enact new laws or treaties to implement the suggestions argued in this Note to minimize the impending risk that cyberspace brings.

This Note concludes that cyberattacks can constitute an act of war when they rise to that level, and suggests how we should respond to such attacks. This Note recommends that international law and treaties adopt this framework—or another akin to it—in order to more confidently face cyberwarfare and its devastating future.

---

[123] *Id.* at 5.

[124] *North Atlantic Treaty Organization (NATO), 1949*, OFFICE OF THE HISTORIAN, https://history.state.gov/milestones/1945-1952/nato [https://perma.cc/XA24-39EU].

VI. CONCLUSION

In a sense, war has not changed. The end results will always remain the same: death and destruction; even if that destruction is not fully tangible. The results may be instantaneous, or they may be delayed. It is only the means implemented to achieve these destructive ends that evolve. Cyberwarfare is a product of that evolution. Most importantly, we must always remain abreast of evolution and the changes in warfare in order to effectively and efficiently respond to new attacks, and to prevent them as well.

This Note sheds light on recent evolution in warfare. It enlightens the reader of the history and science behind cyberattacks through recent incidents involving cyber; argues that cyberattacks can constitute an act of war in international law by triggering the right to self-defense; proposes a tiered analysis in order to effectively, proportionally, and legally respond to attacks in cyberspace; and recommends that the international and national community take the necessary measures to implement this suggestion in order to prepare for the inevitable: a devastating cyberattack.