RUTGERS
JOURNAL OF LAW & PUBLIC POLICY

VOLUME 17 FALL 2019 ISSUE 1

About the Rutgers Journal of Law & Public Policy

The *Rutgers Journal of Law and Public Policy* (ISSN 1934-3736) is published three times per year by students of the Rutgers School of Law – Camden, located at 217 North Fifth Street, Camden, NJ 08102. The views expressed in the *Rutgers Journal of Law & Public Policy* are those of the authors and not necessarily of the *Rutgers Journal of Law & Public Policy* or the Rutgers School of Law – Camden.

Form: Citations conform to *The Bluebook: A Uniform System of Citation* (20th ed. 2016). Please cite the *Rutgers Journal of Law & Public Policy* as 17 RUTGERS J.L. & PUB. POL'Y __ (2019).

Manuscripts: The *Rutgers Journal of Law & Public Policy* seeks to publish articles making original contributions in the field of public policy. The *Journal* accepts both articles and compelling essays for publication that are related to the expansive topic of public policy. Manuscripts must contain an abstract describing the article or essay which will be edited and used for publication on the website and in CD-ROM format. The *Journal* welcomes submissions from legal scholars, academics, policy makers, practitioners, lawyers, judges and social scientists.

Electronic submissions are encouraged. Submissions by email and attachment should be directed to submissions@rutgerspolicyjournal.org.

Paper or disk submissions should be directed to *Rutgers Journal of Law & Public Policy*, Rutgers University School of Law – Camden, 217 North Fifth Street, Camden, New Jersey 08102.

Subscriptions: Subscription requests should be mailed to *Rutgers Journal of Law & Public Policy*, Rutgers University School of Law – Camden, 217 North Fifth Street, Camden, New Jersey 08102, or emailed to info@rutgerspolicyjournal.org.

Internet Address: The *Rutgers Journal of Law & Public Policy* website is located at http://www.rutgerspolicyjournal.org.

OFFICERS OF THE UNIVERSITY

LAW SCHOOL ADMINISTRATION

PROFESSORS OF LAW EMERITI

FACULTY

RUTGERS
JOURNAL OF LAW & PUBLIC POLICY

VOLUME 17 FALL 2019 ISSUE 1

Current Issues
in Public Policy

ISSN 1934-3736

Sorting Solutions: The Fix to the International Legal Framework on Cyberwarfare and Cyberterrorism is a Decision Tree, Not a Magic Bullet

E. Claire Newsome[1]

[1] The author wishes to give a special thank you to her research advisor, Dr. Adnan Zulfiqar. Some of the materials in Part D on attribution were taken from the author's Jessup International Moot Court memorial.

Table of Contents

I. Introduction

The internet is an international wild west.[2] Cyberattacks, such as the Russian hacking of the Democratic National Committee ("DCC") and Democratic Congressional Campaign Committee ("DCCC") private servers, are becoming more prevalent and easier to implement.[3] Arising with the prevalence of cyberattack are concerns that international law is not apt to defend against them or punish them. Defining the new problems presented by cyberattacks and finding a solution to address them has become a preeminent goal of international legal scholars.[4] Typically, the scholarship defines problems individually and then addresses why a single solution will help one or all of those problems.

Such a piecemeal approach creates a division. Some scholars argue for adapting existing international law to encompass solutions for cyberattacks and others argue that we need a new international legal system to deal with harm committed in cyberspace. More division lies

[2] Alexander J. Martin, *GCHQ chief: Cyber conflict could deteriorate into a Wild West if left unchecked*, SKYNEWS (Feb. 25, 2019 8:46 PM), https://news.sky.com/story/gchq-chief-cyberconflict-could-deteriorate-into-a-wild-west-if-left-unchecked-11647971; *see also* Olivia Butler, *Letter: Where to draw the line on free speech on the internet?*, MERCURY (Mar. 3, 2019), https://www.pottsmerc.com/opinion/letter-where-to-draw-the-line-on-free-speech-on/article_85670e7c-3c52-11e9-940e-9390e882faa8.html.

[3] Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE J. INT'L L. 191, 199 (2018) ("there have been countless [] denial-of-service and malware attacks with [] devastating consequences.").

[4] Borka Jerman-Blažic & Tomaž Klobucar, *Missing Solutions in the Fight against Cybercrime and Cyberterrorism – the New EU Research Agenda*, IEEE COMPUTER SOC.: 2016 EUROPEAN INTELLIGENCE & SEC. INFORMATICS CONF., 2016, at 128, DOI 10.1109/EISIC.2016.16.

within the attribution problem. Since cyberattackers easily obscure their identities, some scholars assert that the international community should lower the standard for attributing attacks to suspects. However, others think resources should be funneled to investigatory institutions to address the attribution problem.[5]

Ultimately, none of these solutions are a magic bullet solution for taming cyberspace. This piece builds a framework that international legal professionals can use to assess which solution is necessary for which problem. Part II introduces the Russian hacking of the DNC and DCCC, which serves as a case study to illustrate the concepts discussed in subsequent parts. Part III defines terrorism and warfare; and identifies the issues that arise with these definitions in cyberspace. It then discusses the attribution problem and why lowering the standard of proof required to attribute an attack to a state will not solve the attribution problem.

Finally, Part IV will provide a framework that can be used to develop international law on cyberterrorism and cyberwarfare moving into the future. It uses a decision-tree model that creates a hierarchy of solutions proffered by scholars. If the initial solution will not be effective on the problem, a subsequent solution should be used, and so on and so forth. At a glance, it suggests that gaps in cyberterrorism and cyberwarfare jurisprudence be filled first by using analogy, then by creating treaties, then by increasing resources to international police organizations, and finally by increasing the power of the international court system.

II. Russian Hacking of the DNC and DCCC, A Case Study.

[5] Toby L. Friesen, *Resolving Tomorrow's Conflicts Today: How New Developments Within The U.N. Security Council Can Be Used To Combat Cyberwarfare*, 58 NAVAL L. REV. 89, 104 (2009).

This note will explore Russia's cyberattack on the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC) as a case study. In July of 2018, twelve Russian military intelligence officers were indicted as perpetrators.[6] The indictment alleged that two years prior, Russian agents launched a cyberattack on Hillary Clinton's email servers and the email addresses of 76 members of her campaign.[7] The agents made up a group called the Main Intelligence General Staff, or the "GRU,"[8] and the indictment alleges these actions were done in an effort to interfere with the 2016 election.[9]

To perpetrate this attack, Russian agents planted malware on the DNC and DCCC's computer systems, allowing them access to emails and documents.**[10]** The hackers allegedly used spearphishing attacks, an advanced phishing attack.**[11]** A spearphishing attack is a more advanced version of a phishing attack. In a simple phishing attack, the hacker sends emails to a victim's email address.**[12]** The email will implant

[6] Ellen Nakashima & Shane Harris, *How the Russians hacked the DNC and passed its emails to WikiLeaks*, WASHINGTON POST (July 13, 2018), https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553.

[7] *Id.*

[8] Indictment at ¶1, United States v. Netyksho, No. 1:18-cr-00215-ABJ, (D.C. Cir. 2018).

[9] *Id.* at ¶2.

[10] *Id.* at ¶4-8.

[11] *Id.* at ¶13.

[12] Nena Giandomenico, *What is Spearphishing? Defining and Differentiating Spearphishing from Phishing*, DIGITAL GUARDIAN (July 15, 2019),

malicious software ("malware") onto the victim's hard drive when the victim opens the email's attachment.[13] The more sophisticated spearphishing attack personalizes the email using information the attacker learns about the victim, usually through publicly available internet sources.[14] This makes it hard for the victim to recognize the email's malicious source until it is too late.[15] In the DNC and DCCC hacking the links in the emails looked like excel files of polling data, a less suspicious pseudo-document than internet links.[16]

The spearphishing emails, according to the indictment, also masqueraded as an email from Google's security team.[17] This method of trickery, where hackers disguise their email address, is called "spoofing."[18] The email claimed there had been a security breach and the DNC victims needed to change their password by clicking on the link.[19] Instead, the link activated malware named "Agent-X," which allowed hackers to access and monitor the computers once installed on the local

https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] Indictment at ¶21(d).

[17] *Id.* at ¶21(a).

[18] Jason Stadtlander, *Email Spoofing: Explained (and How to Protect Yourself)*, THE HUFFINGTON POST (Jan. 16, 2015 12:06 PM), https://www.huffingtonpost.com/jason-p-stadtlander/email-spoofing-explained-_1_b_6477672.html.

[19] Indictment at ¶21(a).

hard drive.[20] It also allowed hackers to make copies of and transfer documents from the DNC and DCCC servers.[21]

Through Agent-X monitoring functions, hackers captured screenshots of victims' computers at the DNC and DCCC.[22] They used proxy servers to run their operations, which allowed them to obscure their locations.[23] The Russian hackers would make a request to the proxy server that sits anywhere else in the world.[24] Then the proxy server would launch the attack.[25] That way, even if the attack could be traced back to the proxy server, it may not be traceable to the hackers' server.[26]

The Russian hackers then released stolen documents to Wikileaks and fabricated accounts claiming to be connected to the conspiracy theories subjects, such as the illuminati.[27] Russian officials gave the hacked emails to Wikileaks envisioning that Wikileaks would release them to the public.[28] They also released information through their own fabricated online accounts, like "Guficer 2.0," and used networks

[20] *Id.* at ¶14.

[21] *Id.* at ¶32-34.

[22] *Id.* at ¶25.

[23] *Id.*

[24] Jeff Petters, *What is a Proxy Server and How Does it Work?*, VARIONS (Feb. 19, 2019), https://www.varonis.com/blog/what-is-a-proxy-server/.

[25] *Id.*

[26] *Id.*

[27] Indictment at ¶35-46.

[28] Nakashima and Harris, *supra* note 6.

around the world to obscure their identities.[29] Further, they timed the more shocking leaks to coincide with important Democratic events.[30]

As investigators and the cybersecurity firm CrowdStrike began investigating the hackers' cyber footprints, clues arose linking the cyberattacks to Russia.[31] For example, Soviet officials had their names embedded in the metadata of the documents released by Gucifer 2.0.[32] The metadata also contained Cyrillic script.[33] Investigators were able to link the hacking techniques to the techniques of hacking groups known to be affiliated with Russia.[34] Moreover, they were able to link the IP addresses and the malware tool encryption keys used against the DNC and DCCC to the same Russian groups.[35] Social clues also gave the Russian hacking group away. For example, the hackers only operated during Russian workday hours and did not operate on Russian holidays.[36]

[29] Indictment at ¶4-8.

[30] *Id.* at ¶48-49.

[31] Max Fisher, *Why Security Experts Think Russia Was Behind the D.N.C. Breach*, N.Y. TIMES (July 26, 2016), https://www.nytimes.com/2016/07/27/world/europe/russia-dnc-hack-emails.html.

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] John Walcott, Joseph Menn, & Mark Hosenball, *U.S. theory on Democratic Party breach: Hackers meant to leave Russia's mark*, REUTERS (July 27, 2016, 8:23 PM), https://www.reuters.com/article/us-usa-election-russia-theory/u-s-theory-on-democratic-party-breach-hackers-meant-to-leave-russias-mark-idUSKCN10801S.

[36] *Id.*

This case presents unique questions. First, while there is a lot of circumstantial evidence, there are no firsthand accounts linking the hacking group to the attacks. Is this circumstantial evidence sufficient to say the Russian hacking groups were responsible for the attacks? Second, the Wikileaks and Gucifer 2.0 document release did not involve a security breach but was a valid use of the internet. Can these actions qualify as a cyberattack? Also, Wikileaks is not an arm of the Russian government, but aided the government in disseminating the hacked documents. This raises the question of whether Wikileaks's acts can be attributed to the Russian government, which is necessary before the Russian government may be held accountable for Wikileaks's document dissemination.

The DNC and DCCC hacking also raises jurisdictional questions. The United States ("U.S.") charged the Russian officials leading this hacking campaign with various crimes in the U.S., however the Russian officials are outside the U.S.'s jurisdiction. Any further justice would have to take place under international law. Does international law provide adequate recourse? Finally, while the cyberattack was intrusive, it did not cause any physical harm. This will affect which legal framework applies to the attack and raises questions about whether the legal frameworks that are excluded should be adjusted so that Russia's attacks fall within their grasps.

III. Defining Malicious Activity in CyberSpace within the Current International Legal Framework

Traditional legal frameworks provide an appropriate starting point for defining cyberattacks. These frameworks, developed over centuries, can boast the wisdom of experience. It is essential to bring this wisdom into cyberspace. In fact, many scholars consider cyberspace an additional terrain on which aggression may occur.[37] Of course, cyberspace is not directly analogous to any terrain, but discrete adaptions are sufficient to remedy the disparities. This piece focuses on cyberterrorism and cyberwarfare in particular.

This section will first define *what* a cyberattack is. After that, it will discuss how cyberattacks can be sorted into the traditional definitions of warfare and terrorism based on *who* perpetrated the attack, the *intent* behind the attack, and the *effects* of the attack. While cybercrime is another developing area, it lies outside the scope of this piece. However, it is important to remember that if an act does not fit the definition of cyberwarfare or cyberterrorism, it will still most likely be a cybercrime.[38] This article focuses on cyberwarfare and cyberterrorism

[37] Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N L. JUD. 602, 603 (2011) (describing that technology has moved warfare from terrain to terrain, notably how the introduction of planes into warfare made nautical warfare less significant).

[38] *See* Susan W. Brenner*, Technological Change And The Evolution Of Criminal Law: "At Light Speed": Attribution And Response To Cybercrime / Terrorism / Warfare,* 97 J. CRIM. L. & CRIMINOLOGY 379, 386 (2007) ("[C]ybercrime is the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order. This definition encompasses both traditional and emerging cybercrimes."); Rebecca Crootof, *International Cybertorts: Expanding State Accountability In Cyberspace*, 103 CORNELL L. REV. 565, 594 (2006) (describing cybercrime as a "violation of criminal law committed by means of computer system" and governed by "[d]omestic and [i]nternational [c]riminal [l]aw."); *but see* Logan Hamilton, *Beyond Ballot-Stuffing: Current Gaps In International Law Regarding Foreign State Hacking To Influence A Foreign Election*, 35 WIS. INT'L L.J. 179, 201 (2017) (arguing that cybercrime is not an adequate framework to address

because categorizing attacks as merely criminal can seem unsatisfying under certain circumstances.

As will be discussed below, the Russian hacking of the DNC and DCCC does not fit snugly into cyberwarfare or cyberterrorism definitions. The hacking of the DNC and DCCC seems like a grave attack on a sovereign nation, so this result may be dissatisfying. Ultimately, the objective of preserving international peace will supersede this dissatisfaction.

A. The Preliminary Task of Defining a Cyberattack.

Before analyzing whether an incident is cyberwarfare or cyberterrorism, it is important to determine whether the incident is a cyberattack in the first place. Cisco, one of the world's leading server security providers and innovators, defines a cyberattack as a "malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization."[39] This approach focuses on the intent and the actions of the individual. The United States Navy takes a different approach, focusing on the act's effects. It defines a cyberattack as "cyberspace actions which create various direct denial effects (i.e. degradation, disruption, or destruction) and manipulation that leads to denial."[40]

Under these theories, it is important to remember, however, that simply using the internet to launch some type of attack does not qualify

the election hacking because of the many cybercriminals that lie outside of victim states' jurisdictional reach).

[39] *What Are the Most Common Cyberattacks?*, CISCO, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

[40] U.S. DEP'T OF THE NAVY, DEPARTMENT OF THE NAVY CYBER GLOSSARY: TERMS AND DEFINITIONS, 4 (2017).

as a cyberattack.[41] For example, Gucifer 2.0 or Wikileaks releasing stolen information via the internet does not qualify as a cyberattack. Although they may have liability for the hacking under a conspiracy case, the release of the information on social media and the Wikileaks site alone did not exploit the infrastructure of the internet. Therefore, it was not a cyberattack even though the internet was used to commit the harm.

Other organizations take a normative approach. Dr. Camino Kavanaugh proposed a normative methodology in a 2017 UNIDR resource report.[42] This methodology aimed to define a cyberattack by "identifying areas of common understanding and divergence on issues relating to cyberspace and international security, notably norm development, legal measures, and possible approaches to the malicious use of cyber tools."[43] Under a norms theory, Gucifer 2.0 and Wikileaks could be liable if their actions violated an established norm.

Ultimately, this piece will use definition offered by United States Navy because it was made with international law in mind[44], unlike the Cisco definition, and is more specific than the UNIDR definition.

B. Defining Warfare and Cyberwarfare.

[41] *Id.*

[42] Camino Kavanagh, The United Nations, *Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*, UNIDIR RESOURCES, 11 (2017).

[43] *Id.* at 33.

[44] U.S. DEP'T OF THE NAVY, DEPARTMENT OF THE NAVY CYBER GLOSSARY: TERMS AND DEFINITIONS, 4 (2017).

Applying traditional principles of warfare in a cyber context, cyberwarfare occurs when a cyberattack is attributable to a state and is capable of causing deleterious effects, such as death or destruction of property.

1. Law of Armed Conflict: Warfare under International Law.

International law divides warfare into two categories. *Jus ad bellum* governs the transition from peace to war.[45] *Jus in bello* governs war-time behavior.[46] Any wartime action must follow the principles of discrimination, distinction, proportionality, and precautionary measures.[47] This section focuses on *jus ad bellum* because it determines whether an act is an act of warfare.[48] There is currently a lot of controversy on how cyberattacks should fit in existing legal frameworks – or whether they should at all.

Article 2(4) and Article 51 of the United Nations Charter ("Charter") are the current principles that define warfare.[49] They are *jus ad bellum* principles, which means they determine when a state's act constitutes an act of war in the absence of an ongoing conflict.[50] However, the principles of warfare, as we know them today, have their roots in the Hague and Geneva Conventions. While the Hague and Geneva

[45] Jessica R. Gross, Note, *Hack and be Hacked: A Framework for the United States to Respond to Non-state Actors in Cyberspace*, 46 CAL. W. INT'L L.J. 109, 128 (2016).

[46] *Id.* at 131.

[47] *Id.*

[48] Gross, *supra* at note 45, at 128.

[49] Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 562-63 (2010).

[50] Gross, *supra* at note 45, at 129.

Conventions govern *jus in bello*, or the legal boundaries that constrain actions taken during a war, the treaties can still inform interpretations of *jus ad bellum* acts.[51]

i. Hague Convention and Geneva Conventions that govern jus in bello.

The Hague Convention was passed in 1907 and aimed to limit the right to injure enemies during wartime.[52] After World War I and World War II, however, the international community believed that the Hague Convention needed expansion.[53] This need led to the creation of the Geneva Conventions.[54] The Geneva Conventions expanded on the Hague Convention to encompass acts not traditionally viewed as war.[55] Instead, it purported to govern "armed conflicts."[56] It also sought to provide further protection to enemy combatants, prisoners of war, civilians, and humanitarian aid providers.[57] The Geneva Protocols of 1977 implemented more defined limitations on wartime conflict.[58] For example, they prohibited weapons that cause unnecessary suffering or chronic damage to the natural environment.[59]

[51] Gervais, *supra* note 49, at 535.

[52] Shaun Roberts, *Applying Conventional Laws Of War To Cyber Warfare And Non-State Actors*, 41 N. KY. L. REV. 535, 535 (2014).

[53] HISTORY CHANNEL, *Geneva Convention,* https://www.history.com/topics/world-war-ii/geneva-convention (last visited on August 21, 2018).

[54] *Id.*

[55] Roberts, *supra* note 49, at 535.

[56] *Id.*

[57] History.com Editors, *supra* note 53.

[58] *Id.*

[59] *Id.*

Although the Geneva and Hague Conventions are not universally adopted, much of their principles are considered binding by force of customary international law.[60] That means that all nations are bound to them when engaging in ongoing wartime conflict. However, they do not determine when the ongoing wartime conflict begins. Article 2(4) and Article 51 of the UN Charter, *jus ad bellum* principles, determine when a state's act rises to an act of war in the absence of an ongoing war.[61]

ii. Jus ad Bellum: Article 2(4) and Article 51 of the UN Charter.

Article 2(4) prohibits states from purveying 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."[62] It is the general consensus that use of force under Article 2(4) is armed force and not other types of force, such as political or economic coercion.[63] Moreover, Article 2(4) only references the use of force by *states*.[64] In other words, unless the conduct of a non-state entity can be attributed to a state, the non-state entity cannot commit an act of war. Applying this to the hack of the DNC and DCCC servers, if the allegations in the indictment are true, the hacking would be

[60] Roberts, *supra* note 49, at 535.

[61] Gervais, *supra* note 49, at 562-63.

[62] U.N. Charter art. 2, ¶ 4.

[63] Oona A. Hathaway, et al., *The Law of CyberAttack,* 100 CALIF. L. REV. 817, 842 (2012); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law- Thoughts on a Normative Framework*, 37 COLUM. J. OF TRANSNAT'L LAW 885, 15 (1999).

[64] Gervais, *supra* note 49, at 546. As discussed below, force purveyed non-state actors may be attributable to a State in a manner that triggers an Article 2(4) "use of force." *Id.*

attributable to Russia because the GRU is a part of the Russian government. But what if instead of using the GRU to hack the private servers, Russia induced an independent hacking group? This is an example of the attribution problem discussed in Section C of Part III.

Customary international law of non-intervention can shed light on the type of act that constitutes a violation of Article 2(4). Customary law prohibits states from interfering with the internal affairs of other sovereign states.[65] In *Nicaragua v. U.S.*, the International Court of Justice ("ICJ") held that if a state violates the customary principle of non-intervention by use of or threat of force, the state has breached Article 2(4).[66] In this holding, the force could be direct or indirect to constitute a violation.[67]

But what is the recourse for an Article2(4) violation? Article 51 provides that states have a right to self-defense only in response to an "armed attack."[68] The UN Charter's self-defense principles shed light on what constitutes an "armed attack" under Article 51. Under the UN Charter, a state can only engage in self-defense out of necessity and the defense must be proportional to the initial armed attack.[69] It may only be used when no other peaceful means are available and only within the

[65] *Id. See also,* G.A. Res. 25/2625, ¶1, U.N. Doc. A/RES/47/1 (Oct. 24, 1970).

[66] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 176 (June 27).

[67] *Id. See also* G.A. Res. 25/2625, *supra* note 63. ("No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.").

[68] U.N. Charter art. 51. Under Article 39 of the Charter, the Security Council may also authorize use of force to "maintain or restore international peace and security." U.N. Charter art. 39.

[69] Hathaway, et al., *supra* note 63, at 849.

scope of the armed attack that triggered the right to self-defense.[70] Moreover, the use of force may not be merely retaliatory or punitive.[71] Therefore, an attack can only rise to the level of an "armed attack" if it produces the most serious of consequences.[72] In fact, the ICJ ruled that an "armed attack" is the gravest offense and a product of effect and intensity.[73]

An Article 2(4) "use of force" is broader than an Article 51 "armed attack."[74] Thus a state may have its rights violated under Article 2(4) of the Charter, but it may not be able to use self-defense under Article 51 of the Charter. This makes sense in light of the Charter's purpose, which is to promote harmony between states.[75] This suggests that retaliation should only be taken where there is no other option. [76] Even if force is used against a state, the state should be challenged to seek out more peaceful means of redress before resorting to self-defense.[77]

2. Cyberwarfare: Applying Traditional Law of Armed Conflict to Cyberattacks.

i. Article 2(4): "Use of force" in Cyberspace.

[70] *Id.*

[71] Walter Gary Sharp, Sr., *CyberSpace and the Use of Force,* AEGIS RESEARCH CORPORATION 1999, 37-38, http://www.thomas hastings.org/CyberSpace%20and%20the%20Use%20of%20Force%20-%20Sharp1999.pdf.

[72] Roberts, *supra* note 52, at 549.

[73] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. at 191 (June 27).

[74] *Id.*

[75] UN Charter, art. 1, ¶ 1.

[76] SHARP, *supra* note 71, at 83.

[77] *Id.*

It is not immediately obvious that cyberattacks constitute a "use of force" under Article 2(4).[78] Again, use of force generally involves the use of military instrumentalities.[79] So, can a cyberattack qualify as unlawful armed force? The answer is yes, as long as it causes a "destructive effect within the sovereign territory of another state."[80] Moreover, scholars classify malware used to commit a cyberattack as a weapon even though it does not fit our traditional conception of weaponry.[81]

The Vienna Convention on the Law of Treaties should be used to interpret "use of force," which provides that treaties will be interpreted according to a good faith understanding of the plain text in the context in which the treaty was ratified.[82] Given that "armed" is used to qualify "force" in the Article's plain language, along with the *travaux préparatoires* of Article 2(4) which show that non-military types of force were considered and rejected, "armed force" is understood to be force perpetrated with the use of military instrumentalities.[83]

[78] Friesen, *supra* note 5, at 101.

[79] Schmitt, *supra* note 63, at 14.

[80] SHARP, *supra* note 73, at 102.

[81] Raboin, *supra* note 37, at 608; Roberts, *supra* note 52, at 541.

[82] Gervais, *supra* note 49, at 536. The Vienna Convention on the Law of Treaties has 116 party states and is adopted by the United Nations. United Nations Treaty Collection, Depository, https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXIII-1&chapter=23&Temp=mtdsg3&clang=_en.

[83] Schmitt, *supra* note 63, at 14. *Travaux préparatoires* are the procedural history of the Article. *Id.* The *travaux préparatoires* of the San Francisco Convention, where Article 2(4) was drafted, shows that economic and political coercion were considered and rejected by a vote of 26-2. *Id.*

So, when does a cyberattack rise to an Article 2(4) "use of force"? There are two prevailing approaches to answering this question. The first, enumerated by Gary Sharp, asks whether the attack's "scope, duration, and intensity" are at a level that qualifies as force.[84] These three factors are applied on a case-by-case basis and weighed against international normative behavior.[85] In light of these factors, Sharp concludes that "any state activity in cyberspace that intentionally cause[s] any destructive effect within the sovereign territory of another state are an unlawful use of force." [86]

The second approach, enumerated by Michael Schmitt, balances the factors that separate armed force from other types of forces, such as economic and political coercion.[87] The factors are *severity* of the attack, the *immediacy* with which the negative consequences occur, the *directness* of the link between the act and the consequences, the *invasiveness* of the act into the rights of the state, the *measurability* of the damage caused by the attack, and the *presumptive legitimacy* of the attack under international law.[88] If upon consideration of the factors the cyberattack looks more like a military attack than economic or political coercion, it constitutes "use of force" under Article 2(4).[89]

[84] SHARP, *supra* note 71, at 7.

[85] Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 A.F. L. REV. 65, 69 (2009). A similar analysis is used in other conventions governing warfare technologies, such as the Chemical Weapons Convention. SHARP, *supra* note 71, at 63.

[86] SHARP, *supra* note 71, at 102.

[87] *Id.* at 7.

[88] Schmitt, *supra* note 63, at 18-19.

[89] *Id.* at 19.

So, in the case of the DNC and DCCC hacking, the attack may not qualify as a use of force under the Sharp test or the Schmitt test. Both tests envision some type of damage done that mirrors the effects of typical kinetic warfare. Under the Sharp test, a cyberattack will qualify as an Article 2(4) attack if it causes destruction.[90] The Schmitt test looks to see if, under the factors, the attack looks more like a kinetic attack than political coercion.[91] However, the DNC and DCCC hacking did not cause the same destruction as typical kinetic warfare and the result of the attack seemed more like political coercion. Therefore, it would not rise to the level of an Article 2(4) attack.

ii. When does a cyberattack rise to an Article 51 "Armed attack?".

There are four prevailing approaches to determining when a cyberattack is grave enough to constitute an Article 51 "armed attack." An instrument-based approach defines an armed attack as any attack perpetrated with or against a network system.[92] A target-based approach defines an armed attack as an attack in cyberspace that targets a country's "critical infrastructure," which includes the structures and systems critical to a nations' well-being.[93] The effects-based approach classifies an attack as an "armed attack" if the harm caused has "deleterious consequences" substantial enough to justify self-defense as envisioned by drafters of Article 51.[94] Finally, the sovereign-based

[90] Todd, *supra* note 85, at 102.

[91] Schmitt, *supra* note 63, at 18-19.

[92] Roberts, *supra* note 52, at 554.

[93] *Id.*

[94] Todd, *supra* note 85, at 69-70.

approach defines an armed attack as an attack that "interferes with a state's right of sovereignty."[95]

Most scholars support the effects-based approach because the other approaches have logical flaws when applied to the laws of war. The instrument-based approach is likely disqualified by Article 41 of the UN Charter.[96] Article 41 states interference with a state's electronic equipment does not constitute an armed attack which disqualifies the instrumentalities approach that looks only to damage done to networks without further analysis of the harm caused.[97] The target-based approach is considered under- and over-inclusive.[98] A cyberattack may target a system that is not critical but still causes devastation, which makes the target approach under-inclusive.[99] It is over-inclusive because the mere penetration of a critical system would then qualify as an "armed attack" justifying war on more frequent occasions.[100] Finally, the sovereignty-based approach never gained traction after it was introduced.[101]

Some scholars advocate for bright-line "causative event" approach to simplify the analysis. The causative event approach criticizes the effects-based approach because the effects-based approach heavily emphasizes the harm aspect of the attack.[102] This is not ideal to

[95] Roberts, *supra* note 52, at 555.

[96] *Id.*

[97] U.N. Charter art. 41.

[98] Hathaway, et al., *supra* note 63, at 154.

[99] *Id.*

[100] *Id.*

[101] Roberts, *supra* note 52, at 535.

[102] Todd, *supra* note 85, at 78.

causative event proponents because the harm of cyberattacks can be vastly different across contexts, making the analysis very fact dependent.[103] An causative event approach solves this problem by specifying the events that constitute an Article 51 "armed attack" in cyberspace, which will generally be similar across different contexts.[104] Considering the effects, causative event proponents argue, is more appropriate when determining a remedy.[105] However, bright-line analyses have the potential to violate the purpose of the Charter and customary international law of war, which is to preserve peace before permitting aggression.[106] Classifying an act as warfare without considering the circumstances makes it more likely that a victim state is permitted to respond with aggression, escalating a situation to violence.

The DNC and DCCC attack would not rise to an Article 51 armed attack because it does meet the standards of the broader Article 2(4) use of force. However, the virus called Stuxnet that the U.S. allegedly sent to an Iranian nuclear plant to infect the computers that operated the centrifuges comes closer.[107] Stuxnet made the centrifuges spin too

[103] *Id.*

[104] *Id.* at 79. Todd identifies the use of a cyberweapon by a State as the act sufficient to trigger an Article 51 "armed attack." *Id.* This creates a bright-line indicator that an act of warfare has been committed and a State has had a right violated. *Id.* at 81.

[105] *Id.* at 78. ("The increase in harm (effect) only increases the level of punishment the offender may face from society and does not influence whether a crime of some sort occurred.")

[106] U.N. Charter art 1, ¶ 1.

[107] Josh Fruhlinger, *What is Stuxnet, who created it and how does it work?*, CS ONLINE (Aug. 22, 2017, 2:39 AM), https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

fast, for too long, and destroyed 1,000 machines in the plant.[108] This may rise to the level of an Article 51 armed attack. Since Stuxnet destroyed 1,000 machines at a nuclear powerplant, there is a strong argument that this is the type of deleterious consequences that justify proportional retaliation. This would trigger Article 51 under an effect-based approach analysis. Moreover, even under an causative event approach, the attack may qualify as the type of event that should trigger Article 51 self-defense justification as it was an encroachment on a sovereign state's nuclear plant and caused destruction of property.

However, the UN Charter's goal of promoting peace between the states may counsel against labeling Stuxnet as a justifying retaliation under Article 51. While Stuxnet risked triggering a meltdown, it ultimately did not. Moreover, certain machines were destroyed but the plant, in its' entirety, was not. Instead of justifying kinetic retaliation, civil remedies would compensate for the damage and stave off a violent conflict.

iii. Arguments Against Broadening the Scope of jus ad bellum.

Some commentators argue that we need a completely new framework that labels cyberattacks as acts of warfare when it would not necessarily be labeled so under a traditional analysis.[109] The argument is essentially to expand the definition to encompass various malicious behaviors in cyberspace. However, the purpose of *jus ad bellum* as laid out in Article 1 of the UN Charter is to strive for "international peace and security"[110] and "promote harmony."[111] Article 51 is intentionally

[108] *Timeline: How Stuxnet attacked a nuclear plant*, BBC, https://www.bbc.com/timelines/zc6fbk7 (last visited Oct. 9, 2019).

[109] Raboin, *supra* note 37, at 637.

[110] U.N. Charter art. 1, ¶ 1.

[111] U.N. Charter art. 1, ¶ 4.

a stringent standard to assure the realization of this purpose. A state may only respond with a kinetic attack when horrible damage has been done, and even so, it must obey the mandates of *jus in bello*.[112] Allowing states to respond to cyberattacks with kinetic force, without requiring that cyberattack rise to the level of an Article 51 "armed attack" as currently defined, will result in a loophole through which violence will flow. Harm on the internet should stay on the internet, where there is the lowest chance that lives will be lost.

Finally, there are plenty of feasible methods to retaliate against cyberattacks without engaging in a kinetic attack. States can counter attack in cyberspace. This is called a hack-back.[113] An independent framework would need to be established to govern hack-backs because

[112] Michelle Maiese, *Jus in Bello*, BEYOND INTRACTABILITY (June 2003), https://www.beyondintractability.org/essay/jus_in_bello. Discrimination and distinction.

[113] Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a CyberAttack*, 20 YALE J. L. & TECH. 376, 399 (2018). *See also* Michael Poznansky &

Evan Perkoski, *Did the U.S. 'hack back' at Russia? Here's why this matters in cyberwarfare.,* THE WASHINGTON POST (Feb. 21, 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/02/21/did-the-u-s-hack-back-at-russia-heres-why-this-matters-in-cyberwarfare/ ("The U.S. government, and the intelligence community in particular, see America's ability to "hack back" as crucial for deterring future cyberattacks."); *but see* Robert Lemos, *Why the hack-back is still the worst idea in cybersecurity*, TECH BEACON, https://techbeacon.com/security/why-hack-back-still-worst-idea-cybersecurity (last visited Oct. 3, 2019) (arguing that hack backs could lead to hasty retaliatory strikes that accidentally target an innocent third party instead of the guilty party).

there is no clear guidance currently.[114] However, the *jus in bello* principles of discrimination and distinction, proportionality, and military necessity can serve as an appropriate starting point to provide states guidance to online retaliation.[115]

C. Defining Terrorism and Cyberterrorism.

Applying the principles of terrorism in the context of a cyberattack, cyberterrorism occurs when a non-state actor commits a cyberattack for the purposes of inducing a state of fear meant to compel a government, a population, or an international organization to take or abstain from certain actions. The current historical moment creates an important opportunity to define cyberterrorism because the definition of

[114] Gross, *supra* note 45, at 120.

[115] Maiese, *supra* note 112. Discrimination and distinction disallow states from attacking an individual who has not independently forfeited human rights by participating in the war. *Id.* This usually limits states to attacking soldiers. *Id.* The unavoidable collateral damage to civilians does not transgress this principle so long as it was unavoidable. *Id.* Soldiers may become noncombatants by surrendering, at which point it is impermissible to harm them. *Id. See also* Mark Maxwell & Richard V. Meyer, *The Innocent Combatant: Preserving Their Jus In Bello Protections*, 5 PENN. ST. J.L. & INT'L AFF. 112 (2017); Protocols Additional to the Geneva Conventions of 12 August 1949, art. 51, Nov. 30, 1993, 17512 U.N.T.S 1125. The principle of proportionality requires states to only use as much force necessary to achieve their goals, which usually means that retaliation should be proportional to the initial attack. Maiese, *supra* note 112. At minimum, the state is not allowed to cause excessive damage. *Id.* The Military Necessity principle disallows attacks that cause unnecessary suffering. Maxwell, *supra* note 115. Therefore, even if the attack is proportional, if there is a less injurious method of achieving the permissible goals, the state is required to use the less injurious method. *Id.*

terrorism itself is still in its genesis.[116] Under the existing concepts of terrorism, the DNC and DCCC attack would not qualify as a terrorist attack because it was perpetrated by a state-actor. The actions of Wikileaks would probably not qualify either because it fails the intent element.

1. Widely Undefined: Terrorism under International Law.

There are currently several different definitions of terrorism, however there is no international consensus.[117] Moreover, states tend to keep international definitions of terrorism broad so that they retain discretion in defining terrorism domestically.[118] The Security Council Resolution 1566, adopted in 2004, offers a definition for terrorism. Under Resolution 1566, a terrorist attack is a criminal act committed with dual intents.[119] The first intent is to cause serious bodily harm, to take someone hostage, or to cause death.[120] The second intent is to terrorize the public or a specific group with the goal of compelling a government or international organization to take, or abstain from taking, an action.[121]

[116] Yaroslav Shiryaev, *Cyberterrorism in the Context of Contemporary International Law*, 14 SAN DIEGO INT'L L.J. 139, 142 (2012).

[117] *Id.*

[118] David P. Fidler, *Cyberspace, Terrorism and International Law*, 21(3) J. CONFLICT & SEC. L. 475 (2016).

[119] S.C. Res. 1566, ¶ 3 (Oct. 8, 2004) ("Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act.").

[120] *Id.*

[121] *Id.*

The dual intents make terrorism different from crime, which is motivated by non-political purposes and lacks the intimidation factor.[122]

This note adopts Resolution 1566's definition because it is the most clear, however it does leave notable holes. First, it does not include property damage on any scale.[123] Second, it does not consider effects independent of the analysis of the underlying criminal act.[124] Finally, the definition does not define the actor. However, there does seem to be a general consensus in the international legal community that terrorism can only be committed by non-state actors.[125] This separates terrorism from warfare.[126]

Other treaties adopt the same general definition with a few notable exceptions. The International Convention for the Suppression of the Financing of Terrorism ("ICSFT"), adopted by the UN in 1999, adds that terrorism cannot be committed by those actively involved in an

[122] Brenner, *supra* note 38, at 387.

[123] *Statement For The Record Worldwide Threat Assessment Of TheU.S.Intelligence Community: Senate Intelligence Comm.*, 115th Cong., 2nd Sess. 11 (2018) (statement of Daniel R. Coats, Director, Nat'l Intelligence) (asserting that "[n]ew technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems."). This suggests that the definition of terrorism be expanded to include acts intended to cause harm to markets, health, and infrastructure.

[124] Since Resolution 1566 does not incorporate an effects analysis in the primary definition of terrorism, if an actor sets off a bomb with the intent to kill and for the purpose of terrorizing a community it is terrorism whether or not the bomb actually kills anyone.

[125] Shiryaev, *supra* note 116, at 151.

[126] Acts of warfare must be attributed to a state.

armed conflict.[127] The Draft Comprehensive Convention Against International Terrorism ("Draft CCIT") adds causing property damage,[128] economic loss,[129] attempted criminal acts,[130] and terroristic threats[131] to the actus reus of terrorism. The Draft Convention was proposed in

[127] International Convention for the Suppression of the Financing of Terrorism art. 2(1)(b), Dec. 9, 1999, 2178 U.N.T.S. 197. [hereinafter "ICSFT"] ("Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.").

[128] Rep. of the Ad Hoc Comm. est. by G.A. Res. 51/210 of 17 December 1996, U.N. Doc A/57/37, annex 2 (Jan. 28 – Feb. 1, 2002), 2 (1)(b), [hereinafter "Draft CCIT"] ("Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or to the environment.").

[129] Draft CCIT, supra note 128, at art. 2(1)(c) ("Damage to property, places, facilities or systems referred to in paragraph 1 (b) of the present article resulting or likely to result in major economic loss[.]").

[130] Draft CCIT, *supra* note 128, at art. 2(2) ("Any person also commits an offence if that person makes a credible and serious threat to commit an offence as set forth in paragraph 1 of the present article.").

[131] Draft CCIT, *supra* note 128, at art. 2(3) ("Any person also commits an offence if that person attempts to commit an offence as set forth in paragraph 1 of the present article.").

1966, but its sweeping definition of terrorism has garnered opposition.[132] Some states believe that it labels revolutionaries as terrorists.[133]

2. Cyberterrorism: Applying Existing Notions of Terrorism to Cyberattacks.

Cyberterrorism is a cyberattack that falls into the definition of terrorism. The cyberattack must be committed by a non-state actor and must include the dual intents discussed above. Scholars also distinguish cyberterrorism from attacks on military infrastructure, attacks on government infrastructure, attacks on privately owned utility infrastructure, and attacks on private internet infrastructure.[134] Moreover, various acts of cyberterrorism can also be distinguished from others based on the sophistication of the attack. Cyberterrorist attacks range from unsophisticated to sophisticated.[135] They also range in structure and can be simple-unstructured, advanced-structured, or complex-coordinated.[136] For

[132] *Overcome Narrow Geopolitical Interests: India At UN On Terror Convention*, NDTV (Oct. 9, 2018 15:06 IST), https://www.ndtv.com/india-news/overcome-narrow-geopolitical-interests-india-at-un-on-terror-convention-1929215.

[133] *Id.*

[134] Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and Int'l Org., Conference on the Law and Econ of Cybersecurity*, GEO. MASON L. SCH., at 5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=566361.

[135] Dorothy E. Denning, *Testimony before the Special Oversight Panel on Terrorism Comm. On Armed Serv. U.S. H.R.*, Geo Univ., May 23, 2000. Simple-unstructured attacks are attacks that require little skill and have remedial strategy skills. *Id.* Advanced-structured attacks exhibit an understanding of various networks and have elementary strategy skills. *Id.* Complex-coordinated attacks have the ability to cause "mass-disruption" and have strategy skills. *Id.*

[136] *Id.* Simple-unstructured attacks are attacks that require little skill and have remedial strategy skills. *Id.* Advanced-structured attacks exhibit an

example, if the DNC and DCCC attack qualified as a terrorist attack, it would be sophisticated because of the sophisticated techniques used and complex-coordinated because it was highly strategic and had the ability to cause mass disruption.

Cyberterrorism and traditional terrorism differ in several ways. First, and perhaps obviously, cyberterrorism involves attacks on computer networks.[137] This makes developed countries that rely heavily on computer networks more susceptible to cyberterrorism.[138] Moreover, like cyberwarfare, cyberterrorism is less expensive making it possible to commit terroristic acts without robust access to resources.[139] Cyberterrorists can also program malicious software that lays dormant for some time before wreaking havoc on its victim network.[140]

Finally, the harm caused by a cyberattack may rarely be intended to cause serious bodily injury, to cause death, or to take hostages. Even if the international community expands the definition of terrorism to include property damage, it is not clear that all forms of cyberattacks would classify as cyberterrorism solely on this technicality. For

understanding of various networks and have elementary strategy skills. *Id.* Complex-coordinated attacks have the ability to cause "mass-disruption" and have strategy skills. *Id.*

[137] Shiryaev, *supra* note 116, at 146.

[138] Aviv Cohen*, Cyberterrorism: Are We Legally Ready?*, 9 J. INT'L BUS. & L. 1, 5 (2010); *see also* Coats, *supra* note 123, at 11 ("We assess that concerns aboutU.S.retaliation and still developing adversary capabilities will mitigate the probability of attacks aimed at causing major disruptions ofU.S.critical infrastructure, but we remain concerned by the increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage.").

[139] Fidler, *surpra* note 118, at 475.

[140] Cohen, *supra* note 138, at 5.

example, would the destruction of a state's essential data count as property damage? If the attacker destroyed data to compel a state's government to take a certain action, the data destruction may escape classification as a terrorist act simply because destroying data does not count as property destruction.[141]

Notably, cyberterrorism is the use of the internet as a means of attack, not the use of a computer or the internet to further a terrorist attack.[142] Activities like spreading propaganda, recruiting through the internet, ordering illicit materials online, or using the internet to post videos of terroristic acts are not cyberterrorism.[143]

Since the DNC and DCCC hacking may be attributed to Russia, it is not an act of terrorism. However, if the actions of Wikileaks are not attributable to Russia, would assisting the Russian government potentially qualify as a cyberterrorist act? It would be challenging to make Wikileaks liable for the physical hacking of the DNC and DCCC servers, because it was not involved in the hack. However, even assuming that the organization is liable under a theory of conspiracy, the terrorism intents are not present. First, Wikileaks did not intend to cause serious bodily harm, to take someone hostage, or to cause death. Second, while there are arguments that Wikileaks meant to terrorize a group of people, its objective was not to compel government officials to take a certain action. Therefore, while Wikileaks's actions might constitute a cybercrime, they would not fit into the definition of cyberterrorism.

3. Modern Goals Concerning the Definitional Development of Cyberterrorism.

[141] This inquiry raises theoretical questions about whether data is property.

[142] Shiryaev, *supra* note 116, at 147.

[143] Fidler, *supra* note 118, at 475.

Since the harm caused by a cyberattack may rarely be intended to cause serious bodily injury, to cause death, or to take hostages, some scholars wish to define cyberterrorism independently from traditional terrorism. Altering the definition of terrorism will suffice to ameliorate this concern. Including commandeering essential infrastructure as a terrorist actus reus will cover malware that targets the physical operation of essential infrastructure.[144] If destruction of essential governmental data is added to the definition, then criminal actors who destroy essential data to cause terror or compel a government will fall into the definition.[145]

However, the present historical moment is ripe for incorporating cyberspace into the consideration of terrorism because terrorism is currently not well defined. Tweaking the definition of terrorism slightly to cover acts committed online is more ideal than starting the law-making process for an entirely new legal regime.[146] However, any additions to the definition cannot be too broad. Terrorism is a serious offense which should be heavily punished, but too broad of a category might extend this punishment to acts that are better categorized as crime.

D. The Attribution Problem: A Legal Standard Problem or a Factual Problem?

Attacks via the internet allow for increased anonymity. An example of this is Russian use of proxy servers, which helped the Russians disguise where the attack on the DNC and DCCC originated. Anonymity causes the attribution problem.[147] Attribution is a determination that

[144] Shiryaev, *supra* note 116, at, 172.

[145] The term "essential data" would need further refinement so that the definition of terrorism is not over broad.

[146] Fidler, *supra* note 118, at 475.

[147] Tran, *supra* note 113, at 381.

a specific party is responsible for an attack.[148] This party could be a state, an organization, or an individual.[149]

The attribution problem is not as present in scenarios where anonymity is less desirable. Cyberterrorism creates less of a problem because terrorists generally claim credit for their attacks.[150] If a terrorist organization does not claim credit for their attack, it will undermine its goal of imposing terror to further a specific purpose.[151] Attribution in typical warfare is easy when the opposing party is wearing a uniform.[152] However, sometimes a state attacks another state with non-state actors ("NSAs"), which requires proof before official attribution can be made.[153]

1. Attributing the conduct of a Non-State Actor ("NSA") to a State.

Attribution is important in the context of cyber warfare. For an act to be considered warfare, it must be attributable to a State as a *de jure* or a *de facto* organ of the state.[154] A *de jure* organ of the state is an

[148] *Id.* at 382. *See also* Friesen, *supra* note 5, at 104 (defining attribution as a two-step process where a state must first locate the perpetrator and then link the perpetrator to the wrongdoing).

[149] Brenner, *supra* note 38, at 407- 08.

[150] *Id.*

[151] *Id.*

[152] *Id.* at 406. *See also* Poznansky & Perkoski, *supra* note 113 ("[S]tates may willingly come clean after attacks to showcase their ability to do harm should a target continue to resist their demands.").

[153] Tran, *supra* note 113, at 382. *See also* Poznansky & Perkoski, *supra* note 113 ("This doesn't alter the fact that [cyberattackers] still operate behind a veil of secrecy.").

[154] Rachael Lorna Johnstone, *State Responsibility: A Concerto For Court, Council and Committee*, 37 DENV. J. INT'L L. & POL'Y 63, 67 (2008).

entity that is recognized under that state's official laws.[155] An entity is a *de facto* organ of the state if it is completely dependent on the state, was acting under the instruction of the state, was sufficiently integrated with the state, or was empowered by the state.[156] A corporation's actions may be attributed to a state but only if it is under close government control.[157] There is no uniform standard of proof required to show attribution, the standard is determined by the court on a case-by-case basis.[158] However, in *Nicaragua v. U.S.*, the ICJ applied required a "clear evidence" standard to show attribution, which serves as a guiding point.[159] This standard does not require absolute certainty and is even a lower than the "beyond a reasonable doubt" standard.[160]

In order to establish dependency that makes an NSA a *de facto* organ, the NSA must be so dependent on the State and "exercise a

[155] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, International Law Commission*, U.N. Doc. A/56/10 (Nov. 2001), art. 4 [hereinafter ""] (providing that 'an organ includes any person or entity which has that status in accordance with the internal law of the State).

[156] *See generally* ILC ASR.

[157] ILC ASR art. 5, Commentary ¶ 2.

[158] Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, 50 TEXAS INT'L L.J. 233, 248-49 (2015).

[159] Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 FLETCHER SEC. REV. 55,

66 (2014).

[160] *Id. But see* Hamilton, *supra* note 38, at 201 (2017) (arguing states should add express "clear and convincing evidence" standards to prove attribution in treaties regarding cyberattacks).

degree of control in all fields as to justify" equating the NSA to the state.[161] The state must also have exercised that control to induce the offense.[162] This is called the effective control test, and the level of control may vary based on the factual circumstances.[163] International courts may also attribute an NSA's actions to its state if the state exercises overall control, which is characterized by control in absence of a specific instruction.[164] However, courts sometimes decline to apply the overall control test because "it stretches too far, almost to breaking

[161] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. at 109 (June 27). *See also id.* at 110 (""Yet, according to Nicaragua's own case, and according to press reports, contra activity has

continued. In sum, the evidence available to the Court indicates that the various forms of assistance provided to the contras by the United States have been crucial to the pursuit of their activities, but is insufficient to demonstrate their complete dependence on United States aid.").

[162] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. at 115 (June 27) ("However, whether the United States Government at any stage devised the strategy and directed the tactics of the contras depends on the extent to which the United States made use of the potential for control inherent in that dependence.").

[163] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. at 115 (June 27) ("For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in thecourse of which the alleged violations were committed.").

[164] Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 124 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997) [hereinafter "*Prosecutor v. Tadic*"].

point, the connection which must exist between the conduct of a State's organs and its international responsibility."[165]

An NSA is also a *de facto* organ if the state instructs the NSA to commit an act[166] or the state later acknowledges and adopts the conduct of the NSA.[167] Further, a *de facto* organ arises through sufficient integration of an entity into the government if the entity is exercising elements of governmental authority in circumstances where the government would need to act.[168] Individuals who are compensated by the state and are acting under direction and supervision of that state are *de facto* organs.[169]

If an NSA is empowered by a state to exercise elements of governmental authority, the state is responsible for the NSA's actions that occur as a result of that empowerment.[170] The NSA must be empowered by an internal law.[171] While the state can still be liable for *ultra vires* actions,[172] the state is no longer responsible if the entity's acts are so far outside of the empowerment that it becomes a personal action.[173]

[165] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶ 406 [hereinafter "*Bosnia v. Serbia*"].

[166] ILC ASR art. 8.

[167] ILC ASR art. 11.

[168] *Id.* at art. 9.

[169] *Bosnia v. Serbia*, 2007 I.C.J. 144.

[170] ILC ASR, *supra* note 148 art. 5.

[171] *Id.* art. 5. cmt. ¶ 7.

[172] ILC ASR art. 7. "Ultra vires" means in excess of or contrary to the authority given. *Id.* at art. 7 cmt. ¶ 13.

[173] *Id.* at art. 7 cmt. ¶ 7.

So, looking at the DNC and DCCC hacking, the GRU would be a *de jure* organ of Russia because it was a part of the Russian government. Conversely, Wikileaks was an independent organization, so it would not pass muster under the overall or effective control tests. Moreover, it was not exercising governmental authority, so its actions cannot be linked to Russia on an empowerment or integration theory. However, there is strong circumstantial evidence that Russia instructed Wikileaks to commit the act. The indictment indicates the hackers coordinated with Wikileaks to release the stolen documents during important Democratic events.[174] This is a strong case for attribution through adoption. If Russia operated any level of control over Wikileaks, it may be liable for Wikileaks's dissemination of the hacked documents.

2. Challenges of Attribution in Cyberattacks.

Perpetrators of cyberattacks have an easier time obscuring their identities and locations, which complicates the attribution problem.[175] The internet works through a communication protocol called Internet Protocol ("IP"). When you open up an internet application, like Google Chrome, Internet Explorer, or Safari, and go to a website, like Twitter, your computer sends an IP request to Twitter's servers. The request is broken up into packets of information. The packets contain routing information which direct your request to Twitter's servers. The information also includes a return address. When Twitter receives the request, it returns its own information packet containing the pixels that need to appear on your screen to show you your Twitter page.

[174] Indictment at 48-49, *Netyksho et. al.*, No. 1:18-cr-00215. *See also* Ella Nilsen, *The Mueller indictments reveal the timing of the DNC leak was intentional*, VOX (July 13, 2018, 2:50pm EDT), https://www.vox.com/2018/7/13/17569030/mueller-indictments-russia-hackers-bernie-sanders-hillary-clinton-democratic-national-convention.

[175] Brenner, *supra* note 38, at 407.

Notice how the address of the computer making the request is not necessary.[176] This allows hackers to "spoof" or alter this information so that it looks like someone else sent it, without jeopardizing the transaction.[177] Hackers can also disguise themselves by remotely asking another computer, or a proxy server, to make the data request.[178] Further, the address relayed is not a physical address, but an IP address. Each computer is assigned a new IP address when it connects to a new network (i.e. when you move from your home Wi-Fi to public Wi-Fi at a café).[179] Therefore the hacker's personal information, in theory, does not need to be transferred to successfully complete a transaction over the internet.

Metadata complicates internet anonymity, however. Software packages usually records basic features about the hacker's identity in metadata. This metadata may expose what language the hackers are using, where the computer first connected to the internet, what operating system they used, and other tiny digital fingerprints.[180] These digital fingerprints can reveal the identity of the hacker. For example, the metadata left behind after the DNC and DCCC attack included Cyrillic script, the names of Soviet officials, and techniques consistent with Russian hacking groups.[181]

[176] Tran, *supra* note 113, at 388.

[177] *Id.* at 389.

[178] *Id.*

[179] Stephanie Crawford and Howstuffworks.Com Contributors, *What is an IP Address*, HOW STUFF WORKS (Jan. 12, 2001.), https://computer.howstuffworks.com/internet/basics/what-is-an-ip-address.htm.

[180] Fisher, *supra* note 31.

[181] *Id.*

3. Lowering the bar, or the burden of proof, to make attribution easier in a cyber context.

Some scholars argue for lowering burdens of proof necessary to prove attribution[182] and justify retaliation, including retaliation under Article 51 of the UN Charter.[183] Certain states are more dependent than other states on the internet which renders them subject to more online attacks.[184] The anonymity of the internet makes it harder for these states to prosecute perpetrators because they cannot attribute the attack to the perpetrator.[185]

Although attribution is hard in cyberspace, it is still possible to gather evidence to carry the attribution burden. Take the Russian hacking of the DNC and DCCC, for example. The Russians led a sophisticated attack on the DCCC and DNC but they were still caught. It seems that political barriers, rather than legal barriers, are preventing the United States from holding Russia accountable.[186] Moreover, Stuxnet

[182] Raboin, *supra* note 37, at 641; Tran, *supra* note 113, at 382.

[183] Tran, *supra* note 113, at 382.

[184] *See generally* Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of The Law of Armed Conflict During A Time of Fundamental Change in The Nature of Warfare*, 60 NAVAL L. REV. 1, 32, 37 (2010) (explaining how modern reliance on the internet "present[s] an opportunity for weaker states to gain an asymmetrical advantage over traditional military powers by engaging in cyber warfare. . . [and i]t is often said that the United States has more to lose from cyber attacks than any other state.").

[185] *Id.* at 35.

[186] Joseph Marks, *The Cybersecurity 202: The big cyber story of 2018: The U.S. hasn't been tough enough on Russian hackers*, POWER POST (Dec. 20, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/12/20/the-cybersecurity-202-the-big-cyber-story-of-2018-

was a sophisticated attack on Iranian nuclear reactors but investigations still point to theU.S.as the source of the attack.[187]

Finally, even if lowering the bar for attribution was achieved, a kinetic attack might not still be appropriate. Article 51 governs when a use of force is allowable and the purpose behind Article 51 is to maintain peace.[188] Any retaliation would still have to follow the *jus in bello* principles of discrimination and distinction, proportionality, and military necessity.[189] A kinetic attack would probably not be an appropriate response to an attack that does not rise to an Article 51 "armed attack".

III. The Decision Tree: A Framework for Developing International Law governing Cyberspace.

The introduction of cyberattacks onto the international stage has left open many questions.[190] One question is how a legal framework should develop to address the international community's concerns on

the-u-s-hasn-t-been-tough-enough-on-russian-hackers/5c1adf641b326b6a59d7b206/ ("Chris Painter, a former State Department cyber coordinator under President Obama, [explains,] 'Yes, there were some sanctions and expulsions [of Russian diplomats], but they were a little late and not really strong enough,' . . . . Those efforts were also 'continually undercut' by President Trump's wavering on whether Russia was responsible for the hacking and influence operation.")

[187] Andrea Shalal-Esa, *Iran strengthened cyber capabilities after Stuxnet: U.S. general*, REUTERS (Jan. 17, 2013, 11:03 PM), http://www.reuters.com/article/us-iran-usa-cyberidUSBRE90G1C420130118.

[188] U.N. Charter art. 51. cmt. ¶4, http://legal.un.org/docs/?path=../repertory/art51/english/rep_orig_vol2_art51.pdf&lang=.

[189] Maiese, *supra* note 112.

[190] Jerman-Blažic & Klobucar, *supra* note 4, at 128.

cyberthreats.[191] However, there is no “magic bullet” solution to fix every issue that the current legal framework has in dealing with cyberattacks. This part will match solutions with problems that arise in the current international conversation. It can be used as a framework to direct international lawmakers to the types of solutions needed for specific types of problems, instead of attempting to create a single legal solution that conflates unique problems.

A. Analogy as the First Resort and a Means to Immediately Establish Rules in Cyberspace.

Some lament that cyberspace is the modern-day version of the lawless wild west.[192] Although cyberattacks may not have the tangible effects we generally associate with warfare, terrorism, and crime, they still have the ability to cause harm. For example, hacking a hospital’s electrical control system can cause the deaths of patients on life support. Or, a cyberattacker may hack the controls on a dam and flood communities downstream. Therefore, cyberattacks can be analogized to existing forms of harm and supplemented with specific legal instruments where necessary. Analogy can be used to adapt the hard-won treaties and the understandings captured in customary international law to the demands of the future. That way, international legal professionals will have immediate legal tools and scholars can focus their resources on finding solutions to the more intractable problems.

For example, an international decision maker, such as the ICJ can analogize the conduct and results of cyberattacks to past harms it has addressed. Under the ICJ’s Statute, which establishes the rules of the court, the ICJ can base decisions on

[191] *Id.* at 131.

[192] Martin, *supra* note 2*; see also* Butler, *supra* note 2.

> a. international conventions, 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. [193]

Within these sources of guidance, there are plenty avenues for recourse. State liability for transboundary environmental harm provides a body of law fit for analogy to harm caused in cyberspace. States are liable for unreasonable transboundary environmental harm caused by completely internal activities.[194] For example, in the Trail Smelter International Arbitration, a smelter[195] in Trail, British Columbia released chemicals in the air that caused environmental damage to wildlife, forests, and farmland in Washington State.[196] The international arbitrator

[193] Stat. I.C.J. art. 38(1).

[194] Jaye Ellis, *Liability for International Environmental Harm*, OXFORD BIBLIOGRAPHIES (Feb. 22, 2018), http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0017.xml.

[195] A smelter melts metals but also releases toxins into the air.

[196] Trail Smelter Arbitration Tribunal (U.S. v. Can., Judgment and Award Trib., 3 R.I.A.A. 1905, art. 1 (1938, 1941) [hereinafter "Trail Smelter Arbitration"].

determined that Canada was liable to America for the transboundary harm caused by the smelter.[197] It adopted the principle of *sic utere tuo ut alilenum non laedas*, or one should not use one's own property to injure another.[198]

The Trail Smelter Arbitration provides powerful international precedent for penalizing transboundary harm. While it considered the effects of a state's activities on another state's environment, the internet can be analogized to the environment. A cyberattack originates in one state's internet environment and travels to another state's internet environment. Therefore, it is ripe for analogy with the Trail Smelter decision. After all, one should not use one's own property to injure another is a broad enough principle to encompass cyberattacks. While this is civil liability, and not a determination of warfare or terrorism, it redresses cyberattacks and obtains compensation for victim states.

Moreover, if the nature of a cyberattack aligns with the result that a treaty on warfare or terrorism is meant to prevent, an international decision maker is permitted to interpret the attack as falling within the treaty. [199] The Vienna Convention on the Interpretation of Treaties allows interpreters to use the plain meaning of the words in the context of

[197] *Id.*

[198] *Transboudary Harm in International Law: Lessons from the Trail Smelter Arbitration* 3 (Rebecca Bratspies & Kent Miller, R. eds., 2009), http://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1238&context=ohlj.

[199] Vienna Convention on the Law of Treaties Signed at Vienna art. 31, May 23, 1969, 1115 U.N.T.S. 331 [hereinafter Vienna Convention] ("1. A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."). The Vienna Convention governs the interpretation of international treaties. *Id.*

the treaty's purpose.[200] That means that a treaty's purpose will play an essential role in resolving ambiguities in the plain language.[201] Under Article 32 of the Vienna Convention the *travaux prepatoires*, or "the property work," may be used for interpretation.[202] If the *travaux prepatoires* suggest a cyberattack violates an existing treaty, an international decision maker may interpret the attack as falling within the treaty.[203]

B. Creating New Treaties to Supplement Existing Law.

New treaties can address the harms that analogy cannot reach. There is a specific need for definitional treaties that set the rules about how to categorize cyberattacks.[204] States will then be assured that in the wake of these cyberattacks they will not have to engage in a fact-based analysis to vindicate their rights.

1. The Importance of Addressing Cyberwarfare in Treaties.

Treaties detailing specific actions that constitute cyberwarfare will provide governments boundaries on permissible and impermissible cyberspace conduct. States have already formed treaties in the areas of "atomic, biological, chemical, and nuclear weapons."[205] As states use

[200] *Id.* The Vienna Convention governs the interpretation of international treaties. *Id.*

[201] Cohen, *supra* note 138, at 12.

[202] Vienna Convention art. 32.

[203] Cohen, *supra* note 138, at 13. Some scholars are concerned that this is not enough to capture all attacks that should rise to the level of cyberwarfare or cyberterrorism. *Id.*

[204] Oona A. Hathaway & Rebecca Crootof, *The Law of CyberAttack* 8 FACULTY SCHOLARSHIP SERIES PAPER 3852 (2012), http://digitalcommons.law.yale.edu/fss_papers/3852.

[205] Gervais, *supra* note 49, at 538.

new technology in dangerous ways, it is only natural that countries advocate legal doctrine that will protect them from that technology.[206]

Of course, a treaty is only binding on states that are parties to that treaty.[207] Therefore, if a non-party state commits an attack detailed in the treaty, the victim state may not have a right to redress. However, treaties are still beneficial in three ways. First, they allow a right where one did not exist in the past.[208] In an international landscape where states cannot even settle on the definition of a cyberattack, it will be easier for a state to negotiate discrete agreements with other states without having to convince the entire international community to agree with it. Second, a state may be in a better position to negotiate one-on-one with other states. A state may offer up a concession that is unrelated to cyberwarfare to get a fellow state to agree to its own definition of cyberwarfare.[209] Finally, if enough states follow the definitions of

[206] *Id.; but see* Sally Terry Green, *The Admissibility of Expert Witness Testimony Based on Adolescent Brain Imaging Technology in the Prosecution of Juveniles: How Fairness and Neuroscience Overcome the Evidentiary Obstacles to Allow for Application of a Modified Common Law Infancy Defense*, 12 N.C. J. L. & TECH. 1, 25 (2010) (arguing that before a treaty is made, the international community must have enough knowledge on the scope of cyberwarfare to create an effective treaty and an effective enforcement strategy to realize the goals of that treaty).

[207] Malcolm Shaw, *Treaty*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/treaty (last accessed November 12, 2019).

[208] Raboin, *supra* note 37, at 664.

[209] *But see* Matthew C. Waxman, *CyberAttacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 457 (2011) (arguing that definitions of cyberwarfare should be built through Article 2(4) and 51 so that the states with more influence cannot corner states with less influence into defining cyberwarfare in ways that are ultimately disadvantageous to them).

cyberwarfare found in treaties those definitions may become part of customary international law.[210] At that point, states who are not parties to the treaty will still be bound by it.

2. The Importance of Addressing Cyberterrorism with Treaties.

Introducing new definitions into existing concepts of cyberterrorism through treaties can ameliorate commentators' concerns that poor definitions of traditional terrorism will prevent enforcers from combatting cyberterrorism.[211] States may redefine terrorism in existing treaties or commit to new treaties with definitions of cyberterrorism. For example, the Europe Cybercrime Convention, a framework that governs the definition of cybercrime in Europe, is a popular candidate for application to cyberterrorism.[212] However, scholars also lament that blurring the lines between cybercrime and cyberterrorism is ill-advised because terrorism and crime have a different mens rea.[213] Blurring the lines makes it harder to distinguish between the two when determining appropriate punishment and societies may wish to punish cyberterrorism more than cybercrime. Either way, this definitional question is ripe for finding a solution through treaty.

3. Treaties Can Remediate the Jurisdiction Problem.

Scholars highlight jurisdiction as a major issue for bringing cyberattackers to justice. Since cyberattackers can launch their attack

[210] Rebecca Crootof, *Change Without Consent: How Customary International Law Modifies Treaties*, 41 YALE J. INT'L L. 237, 243 (2016). International norms become customary international law when 1) states practice that norm consistently and 2) states practice that norm under the belief they are legally bound to practice that norm, which is called *opinion juris*. *Id.* at 242.

[211] Shiryaev, *supra* note 116, at 142.

[212] Cohen, *supra* note 138, at 32.

[213] *Id.* at 33.

remotely, there may never be an opportunity for states to apprehend the attacker while the attacker is within jurisdictional reach.[214] However, treaties may help solve this issue. A treaty can be drafted to compel extradition or define adequate local remedies for states and people who are victims of cyberattacks. If a particular state refuses to ratify such a treaty, there could be a provision in the treaty that compels all of the party states to render sanctions if the non-party states do not properly aid in apprehending cyberattackers or provide adequate local remedies.

4. The Importance of De Minimis *Exceptions to Definitions in Treaties.*

Scholars are rightfully concerned that bright line definitions in treaties will create seemingly arbitrary categorizations.[215] Clear *de minimis* exceptions to these definitions can help rectify this concern. A *de minimis* exception ensures that states do not resort to violent remedies after being victimized by a cyberattack when the attack did not render violent harms. International courts and arbitrators would be justified in incorporating *de minimis* exceptions in assessing violations to promote peace and humanitarian goals, especially because the purpose of the UN Charter is to strive for "international peace and security."[216] Moreover, *de minimis* exceptions serve the customary international law mandate of proportionality. This principle requires states to only respond to attacks with a level of force necessary to achieve legal objectives.[217] A *de mimimis* exception will make any treaty definition of cyberwarfare comply with this international mandate.

De minimis exceptions are also crucial when considering cyberterrorism definitions. Too broad of a categorization may mean criminal

[214] Raboin, *supra* note 37, at 645.

[215] Shiryaev, *supra* note 116, at 149.

[216] U.N. Charter art. 1, ¶ 1.

[217] Maiese, *supra* note 112.

implications for freedom of expression and whistleblowers.[218] Defining terrorism must strike a balance between several core human rights. Initially, a definition must protect human rights such as life, liberty, and physical integrity.[219] Terroristic acts directly threaten these rights. However, a legal definition of terrorism must refrain from prohibiting acts that are critical human rights. For example, a law criminalizing the incitement of terrorism may infringe on freedom of expression.[220] These concerns apply in the cyber context as well. For example, labeling the release of government documents acquired over a network as terrorism may be infringing on whistleblowers ability to disseminate critical information to the public.[221]

[218] *Overcome Narrow Geopolitical Interests*, *supra* note 132; *see also* Office of the United Nations High Commissioner for Human Rights, *Human Rights, Terrorism and Counter-terrorism,* 41-42, Fact Sheet No. 32. Additionally, labeling certain groups terrorist groups may stifle freedom of association by limiting people's ability to associate with others without violating international terrorism laws. *Id.* at 43-44.

[219] *Id.* at 7. The right to life is the most important human right because in order to enjoy any other human right, one must be alive. *Id.* at 8.

[220] *Id*. at 41-42. Additionally, labeling certain groups terrorist groups may stifle freedom of association by limiting people's ability to associate with others without violating international terrorism laws. *Id*. at 43-44.

[221] *See* Johan Lidberg, *New bill would make Australia worst in the free world for criminalising journalism*, THE CONVERSATION (Jan. 31, 2018 10:18 PM EST), https://theconversation.com/new-bill-would-make-australia-worst-in-the-free-world-for-criminalising-journalism-90840 ("Our main conclusions are that the current fear-driven security environment has made it much harder for investigative journalists to hold governments and security agencies accountable. This is partly due to anti-terror and security laws making it harder for whistleblowers to act."). *See also* Joshua Birch, et. al., *The State of*

De minimis exceptions can help strike this balance. They introduce a level of discretion for international courts to account for harm in their determinations. If the harm is pro-social, like in the case of whistle-blowing, or if criminalizing the harm will create detrimental precedent to the critical human right, like a suppression of freedom of expression, it will not qualify as a legal wrong. *De minimis* exceptions allow space for treaties to adapt to context.

C. Increasing Investigatory Capability to Solve the Attribution Problem.

Increasing investigative capabilities will help attribute attacks to state actors so victim states may have their interests vindicated under new and existing international law. The attribution problem, as described above, occurs where anonymity over the internet allows states to attack other states without investigators being able to explicitly attribute the attack to the aggressor state.[222] Some scholars suggest lowering the evidentiary standard required to attribute an attack to a state. [223] However, lowering evidentiary standards will increase the amount of false positives which could lead to retaliatory actions against innocent states.[224] Also, it will disincentivize the international community from developing its investigatory capabilities and incentivize attackers to enhance their obfuscation techniques.

Whistleblower & Journalist Protections Globally: A Customary Legal Analysis of Representative Cases, Sch. of Int'l Serv. Am. Univ., 36 (2015) (indicating that Nigeria's anti-terror laws criminalizes "receipt or provision of information or moral assistance, including invitation to adhere to a terrorist or terrorist group" to support for terrorist groups" as terrorism which restrict journalistic freedom).

[222] Tran, *supra* note 113, at 381.

[223] Raboin, *supra* note 37, at 641; Tran, *supra* note 107, at 382.

[224] Schmitt & Vihul, *supra* note 159, at 66.

Instead of relaxing the legal standard for attribution, the international community should improve the institutions that currently combat cybercrime. Critics challenge proposals to increase international cooperation because it asks states to cede some of their sovereignty and provide increased transparency to the international community, including their regional rivals.[225] However, cooperation endues a social expectation that states will act in good faith. Through cooperation, states can decide what rules govern the wild west of the internet without increasing the risks of nations warring over cyberactivity.

1. Using an Investigatory Body to Solve the Attribution Problem.

Increasing funding to the cybercrime units of international investigators will help solve the attribution problem. [226] INTERPOL, an international police force, is an excellent candidate. It provides support to local police to "enable police to work directly with their counterparts, even between countries which do not have diplomatic relations."[227] 194

[225] David A. Sadoff, *How Law Enforcement Cooperation Abroad is Pivotal to Sustainable Development at Home*, 35 B.U. INT'L L.J. 337, 367 (2017).

[226] *See also* Friesen, *supra* note 5, at 121-122 (recommending that the Security Council's Counter Terrorism Committee create a "Subsidiary Body" tasked with enforcing the Security Council Resolution 1373, which puts stringent requirements on counter terrorism measures states must take within their territory).

[227] *What is INTERPOL*, INTERPOL, https://www.interpol.int/en/Who-we-are/What-is-INTERPOL, (last visited Oct. 4, 2019). Article 3 of its Constitution does not allow it to investigate matters that are "political, military, religious or racial character." G.A. Doc. I/CONS/GA/1956, Constitution of the ICPO-INTERPOL, art. 3 (2017) [hereinafter "INTERPOL Constitution"]. This bolsters the argument to keep cyberattacks out of the realm of warfare. Otherwise, INTERPOL would not be able to investigate them under its charter and there will be less solutions open to injured states, other than going to war.

countries are members of INTERPOL[228] and member countries fund its operations.[229] Article 2 of INTERPOL's Constitution defined its purpose as "prevention and suppression of ordinary law crimes."[230] However, INTERPOL does not investigate terrorism but it does have a specific branch to investigate cybercrime.

Unfortunately, INTERPOL's 2017 Financial Report indicated INTERPOL

> . . . faces constraints as regards the availability of qualified staff in some of the more difficult areas of its policing operations, such as cybercrime or terrorism, where experts are difficult to find and/or the few existing experts are in demand elsewhere. These staff shortages expose the Organization's strategy implementation to considerable risks, which are not easily mitigated.[231]

If INTERPOL is provided with more funding by its 194 constituent countries, it will be better situated to prevent and investigate cyberattacks.

INTERPOL may also help solve the jurisdiction issue.[232] While states may be reluctant to grant jurisdiction to other states to seek

[228] *Member Countries*, INTERPOL, https://www.interpol.int/Who-we-are/Member-countries, (last visited Oct. 4, 2019).

[229] *Our Funding,* INTERPOL, https://www.interpol.int/Who-we-are/Our-funding, (last visited Oct. 4, 2019).

[230] INTERPOL CONST. art. 2.

[231] INTERPOL, ANNUAL FINANCIAL REPORT, at 34 (2017).

[232] Raboin, *supra* note 37, at 645.

remedies, they may be more willing to allow INTERPOL jurisdiction because each state is represented in INTERPOL.[233] Moreover, the cyberweapons that attackers use can be a wealth of information without an investigator even needing to step foot into a sovereign nation's territory.[234]

However, new legal principles must be instated to govern the investigators. While investigations are important, empowering police forces oftentimes leads to inequity in policing. Police organizations may pursue a less powerful state implicated in a cyberattack more vigorously than a similarly implicated powerful country. Therefore, precautions need to be taken to ensure international police forces enforce the law equally.

Transparency would also need to accompany empowerment of these forces. For example, INTERPOL's governing body is its General Assembly, a body comprised of delegates from each member state.[235] The General Assembly elects a President who "provides guidance and direction."[236] The General Assembly and President should be held accountable as overseers and have a hand in preventing policing abuses.

2. Treaties on Mutual Assistance Will Also Increase Investigatory Ability.

[233] Friesen, *supra* note 5, at 125 (discussing how a neutral investigatory body would command more authority and legitimacy).

[234] Take the digital footprints left during the DNC and DCCC hacking, for example.

[235] *General Assembly*, INTERPOL, https://www.interpol.int/Who-we-are/Governance/General-Assembly (last visited Sept. 14, 2019).

[236] *President*, INTERPOL, https://www.interpol.int/Who-we-are/Governance/President (last visited Sept. 14, 2019).

Another way to address the attribution problem is to increase the international community's requirements on mutual assistance. Treaties on mutual assistance bind states to base-level cooperation obligations in fighting certain types of crime. The European Convention on Cybercrime is the world's leading mutual assistance treaty on mutual cooperation in combating cyberattacks. It requires its member states to take whatever measures necessary to preserve evidence related to a cybercrime that may have left traces within its boundaries.[237]

There are also multinational taskforces aimed at opening discussion about cybersecurity. For example, the Council for Security Cooperation in the Asia Pacific meets as an "informal mechanism for scholars, officials and others in their private capacities to discuss political and security issues and challenges facing the region."[238] Member countries include "Australia, Brunei, Cambodia, Canada, China, Europe, India, Indonesia, Japan, DPR Korea, Korea, Malaysia, Mongolia, New Zealand, Papua New Guinea, Philippines, Russia, Singapore, Thailand, United States of America and Vietnam."[239] It increases regional security through "dialogues, consultation and cooperation."[240] Opening

[237] Susan W. Brenner & Joseph J. Schwerha VI, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMP. & INFO. L. 347, 361 (2002).

[238] *Home,* COUNCIL FOR SECURITY COOPERATION IN THE ASIA PACIFIC, http://www.cscap.org/ (last visited Sept. 14, 2019).

[239] *Member Committees,* COUNCIL FOR SECURITY COOPERATION IN THE ASIA PACIFIC, http://www.cscap.org/index.php?page=member-committees-page (last visited Sept. 14, 2019).

[240] *About Us,* COUNCIL FOR SECURITY COOPERATION IN THE ASIA PACIFIC, http://www.cscap.org/index.php?page=about-us (last visited Sept. 14, 2019).

dialogues in the region has allowed member states to strategize about threats and create policies to govern international internet use.[241]

The United Nations has also issued recommendations on mutual assistance requirements. The General Assembly's 2000 "Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century" urges member states to increase interstate cooperation on fighting crime in general.[242] While the Resolution addresses crime generally, it emphasizes the "need to develop and promote technical cooperation activities to assist States in their efforts to strengthen their domestic criminal justice systems and their capacity for international cooperation."[243] Combatting cybercrime requires technical cooperation so anything promoting that goal is useful.

D. The Enforcement Problem: International Court Systems as a Legitimizer of Enforcement.

In order for any legal solution to the problems created by cyberattacks to be effective, there needs to be an adequate forum of enforcement. Empowering the international court system to hold states accountable for harms they cause on the internet addresses this concern. The ICJ is especially apt for the task. Any member state of the United Nations is entitled to appear in front of the court, and the General

[241] *Memoranda,* COUNCIL FOR SECURITY COOPERATION IN THE ASIA PACIFIC, http://www.cscap.org/index.php?page=memoranda (last visited Sept. 14, 2019).

[242] G.A. Res. 187/4, 2001 Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, ¶ 4 (Apr. 15, 2001).

[243] *Id.*

Assembly has the ability to grant non-members access to the court.[244] The ICJ gains jurisdiction over international disputes by special agreement, where the parties agree to appear in front of the court, through provisions in treaties that grant the ICJ jurisdiction over any dispute arising under that treaty, and through compulsory jurisdiction, where certain states agree to answer to the court whenever another state wishes to settle a dispute there.[245]

Some argue that the ICJ is too weak to address cyberattacks because its jurisdiction relies upon consent.[246] However, this issue plagues every conflict under international law. The solution is to strengthen the ICJ, not to lower the bar for states to take unilateral action against other states in the event that there is a cyberattack. Although it is challenging to convince states to agree to a stronger court, having recourse for cyberattack may incentivize even the most powerful states to consent to the ICJ's jurisdiction in a special agreement. Also, provisions in new treaties concerning cyberattacks can designate the ICJ as the appropriate forum should a dispute arise under that treaty. Moreover, the ICJ already requires states to take responsibility over internet infrastructure that reside within their territories.[247] It has already addressed issues concerning cyberspace and is an apt place to address such issues in the future.

[244] *States not members of the United Nations parties to the Statute,* INTERNATIONAL COURT OF JUSTICE, https://www.icj-cij.org/en/states-not-members (last visited Sept. 14, 2019).

[245] *Basis of the Court's Jurisdiction*, INTERNATIONAL COURT OF JUSTICE, https://www.icj-cij.org/en/basis-of-jurisdiction (last visited Sept. 14, 2019).

[246] Tran, *supra* note 113, at 406.

[247] Gross, *supra* at note 45, at 120.

Further, ICJ decisions create enforcement options. The treaties created to address cyberattacks can provide that party states must sanction any state who violates an act prohibited in the treaty regardless of whether that state is a party to the treaty. An ICJ ruling can legitimize these sanctions and convince the other states to fulfill their obligations under the treaty. Moreover, an ICJ adjudication can urge the Security Council to impose sanctions on the offending party under its Article 41 powers.[248] These are better options than having states unilaterally retaliate under relaxed international legal standards.[249]

IV. Conclusion

The proliferation of cyberattacks into international affairs has raised many questions. Cyberwarfare introduces the question of when a cyberattack justifies retaliation. However, expanding the definition of warfare to include cyberattacks that do not mirror the effects of traditional warfare incentivizes violent retaliation where peaceful means should otherwise be pursued. Cyberterrorism also presents challenging questions. Since cyberattacks have the potential to cause devastating effects to markets and infrastructure, the definition of terrorism should perhaps be expanded beyond acts intended to cause death or serious bodily injury to include these effects. Defining terrorism is still in its genesis so there is ample opportunity to incorporate cyberattacks into the fold.

[248] *Sanctions,* UNITED NATIONS SECURITY COUNCIL, https://www.un.org/securitycouncil/sanctions/information (last visited Sept. 14, 2019).

[249] G.A. Res. 25/2625, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, ¶ 1 (Oct. 24, 1970) ("Every State shall settle its international disputes with other States by peaceful means in such a manner that international peace and security and justice are not endangered.").

Moreover, the efficacy of attribution law has been questioned in the advent of cyberattacks. It is harder to attribute cyberattacks to the perpetrator, so some have suggested lowering the legal standard. However, this idea runs the risk of incentivizing retaliation against innocent parties. It also disincentivizes the development of investigation into cyberattack.

There are many excellent solutions proffered by scholars to solve the various problems that arise in cyberspace. This article has offered a framework to guide the development of international law as it pertains to cyberspace. First, analogy should be used where possible to fit cyberattacks into existing legal frameworks. This will provide immediate solutions and allow legal scholars to focus on issues where the law does not fit. Second, treaties should be used to plug the holes in existing international law. Third, investment should be made in international investigatory bodies and mutual assistance committees to address the evidentiary issues that arise in cyberspace. This speaks especially to the attribution problem. Finally, enforcement mechanisms, namely sanctions bolstered by international court review, need to be included in any legal solution lacking adequate incentive to be self-enforcing. Ultimately, the newness of cyberspace regulation creates a unique opportunity to incentivize peaceful solutions to wrongs committed via the internet. While it is tempting to provide strict physical consequences for activities in cyberspace, perhaps conflict on the internet should stay on the internet.