THE INADEQUACY OF INTERNATIONAL LAW TO ADDRESS CYBER-ATTACKS IN THE AGE OF ELECTION-MEDDLING

*Brooke Bentley**

* Brooke Bentley is a Spring 2021 graduate of the University of Houston Law Center

INTRODUCTION

War in its traditional sense has existed for thousands of years.[1] As a result, there is a well-established set of international laws governing warfare between nations that have developed over time.[2] In recent decades, however, countries have begun utilizing cyber-space to attack other countries, sometimes simply for information but other times to intentionally disrupt society, perhaps to a political or economic end.[3] Because this "cyber-warfare" is vastly different in several respects from traditional

1. Claudio Cioffi-Revilla, *Origins and Evolution of War and Politics*, 40 INT'L STUD. Q. 1, 4 (1996) (discussing that war was first reliably documented around 3000 B.C. in Mesopotamia).

2. *See generally* G.A. Res. 56/83, at 1 (Jan. 28, 2002) (explaining the significance of the continued development of international law); U.N. Charter art. 1–2 (discussing peaceful relations, restraint from use of force, and other rules among nations regarding the resolution of international conflicts).

3. *See generally Significant Cyber Incidents*, CENTER FOR STRATEGIC & INT'L STUD. (CSIS), https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited Jan. 20, 2021) (providing a list of major international cyber-attacks since 2006 committed for various purposes). *See also Heritage Explains: The Growing Threat of Cyberattacks*, THE HERITAGE FOUND., https://www.heritage.org/node/3646873/print-display (last visited Jan. 28, 2021) [hereinafter *Heritage Explains*] (detailing various instances of nations committing cyber-attacks on others to cause disruptions to their political and economic systems).

warfare, the pre-existing rules governing warfare are inadequate in a variety of ways.[4] Although the drafters of these laws were meticulous and mindful, they simply did not have the foresight to know cyber-attacks would ever even exist. As a result, technology seems to have outpaced the law.

The United States is frequently targeted in these attacks, and cyber-attacks committed against the U.S. are now becoming not only more frequent, but also more complex.[5] Thus, it is imperative that the U.S. work with the international community to create clear and consistent international laws that could also apply to cyber-attacks. Without such guidelines, countries ("states") cannot be held legally responsible by the international community for the effects of cyber-attacks. Although cyber-attacks are usually less physical than traditional acts of war, cyber-attacks can result in both physical damage (like power-grid hacking) and infrastructure damage (such as influencing a country's political culture and electoral outcomes).[6] Therefore, they can be just as destructive as traditional war and should not be ignored.

First, this paper will introduce the pre-existing terminology and international legal frameworks relevant to cyber-warfare as well as briefly discuss the current state of international discussions on this very topic. Second, it will discuss the different

---

4. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 820 (2012).

5. *Heritage Explains*, *supra* note 3 ("No threat facing America has grown as fast, or in a manner as difficult to understand, as the danger from cyberattacks."); *see also* Naveen Goud, *List of Countries Which Are Most Vulnerable to Cyber Attacks*, CYBERSECURITY INSIDERS, https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/ (last visited Jan. 20, 2021) (documenting the United States as the country most targeted by cyber espionage); *Top Daily DDoS Attacks Worldwide*, DIGITAL ATTACK MAP, https://www.digitalattackmap.com/#anim=1&color=0&country=US&list=0&time=17954&view=map (last visited Jan. 20, 2021) (showing the United States as one of the most active countries both as a source and destination of the attacks).

6. *See, e.g.*, Jonathan Fildes, *Stuxnet Worm 'Targeted High-Value Iranian Assets'*, BBC NEWS (Sept. 23, 2010), https://www.bbc.com/news/technology-11388018 (discussing "Stuxnet," the first computer virus known to be capable of specifically targeting and destroying industrial systems such as nuclear facilities and power grids); Michael Wines & Julian E. Barnes, *How the U.S. is Fighting Russian Election Interference*, N.Y. TIMES (Aug. 2, 2018), https://www.nytimes.com/2018/08/02/us/politics/russia-election-interference.html?searchResultPosition=5 ("Moscow's strategy, [the director of national intelligence] said, is to exacerbate sociopolitical divisions.").

types of cyber-attacks that states utilize, specifically focusing on attacks on elections. Third, it will point out the shortcomings of pre-existing international law when applied to cyber-attacks, and recommend how these laws should be modified in order to fill these important gaps.

I. BACKGROUND

Cyber-attacks and cyber-warfare do not occur on a physical battlefield. Rather, they occur in cyberspace—an intangible electronic space with no physical boundaries.[7] Because those that drafted the international laws of war did not contemplate this type of warfare, these pre-existing laws are largely incompatible with cyber-attacks and cyber-warfare.[8] Thus, it is imperative that countries come together to create a more effective legal framework, with the United States leading the way.[9] As will be discussed below, there are several competing views on how the law should be changed, and this paper will address why the U.S. view should be adopted. The U.S. has a large interest in the subject because it is currently facing cyber-attacks on its elections.[10] Russia previously targeted U.S. elections in 2016, and China's recent behavior indicates that it may plan to do the same in future elections.[11] Without an effective set of international laws to govern attacks like these, the U.S. has no legal avenue to deter

7. *See Information Technology–IT Security Techniques–Guidelines for Cybersecurity*, ISO ONLINE BROWSING PLATFORM, https://www.iso.org/obp/ui/#iso:std:iso- iec:27032:ed-1:v1:en (last visited Jan. 28, 2021) (defining "cyberspace" as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.").

8. Hathaway et al., *supra* note 4, at 840–41.

9. It does seem the U.S. is attempting to be an active player in the discussions. *See* Michele G. Markoff, *Office of the Coordinator for Cyber Issues*, U.S. DEP'T OF STATE https://www.state.gov/remarks-and-releases-office-of-the-coordinator-for-cyber-issues/ (last visited Jan. 20, 2021).

10. Wines & Barnes, *supra* note 6.

11. Abigail Abrams, *Here's What We Know So Far About Russia's 2016 Meddling*, TIME (Apr. 18, 2019, 08:20 AM), https://time.com/5565991/russia-influence-2016-election/; *see also* IISS, ASIA PACIFIC REGIONAL SECURITY ASSESSMENT 2019: CHINA'S CYBER POWER IN A NEW ERA 88–89 (May 2019) [hereinafter ASIA PACIFIC REGIONAL SECURITY ASSESSMENT 2019] (explaining how due to recent Chinese election interferences in Thailand and China, there are concerns that China will meddle with US elections).

such cyber-attacks or to hold responsible those that commit such acts.

To date, no multilateral international conventions on cyber operations have been created, and there is disagreement between western countries and countries like China and Russia as to how the law should be changed.[12] The most significant gathering to date has been the U.N. Governmental Group of Experts (GGE). In 2013 and 2015, this group made groundbreaking progress, including agreeing that international law and the state responsibility principles of sovereignty and non-intervention apply to countries' cyberspace.[13] However, when it came to taking action on these discussions, the 2016–2017 U.N. GGE meeting was unable to agree on a consensus report on these issues, with some countries (such as the U.S.) objecting to the application of use of force law to cyber-attacks.[14] Notably, the U.S. felt the proposed report inadequately addressed how international humanitarian law, international law governing the right to self-defense, and the law of state responsibility would apply to states' use of "information communication technologies" (ICTs).[15] Mainly, it feared that an unclear position on these issues would

12. Keiko Kono, *Briefing Memo: International Laws on Cyber Attacks that Do Not Constitute an Armed Attack*, NAT'L INST. FOR DEF. STUD., http://www.nids.mod.go.jp/english/publication/briefing/pdf/2017/briefing_e201710.pdf (last visited Feb. 18, 2021).

13. HARRIET MOYNIHAN, The Application of International Law to Cyber-Attacks: Sovereignty and Non-Intervention 8 (2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.

14. *Id.* at 52; *see also* Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ (noting the United States Deputy Coordinator for Cyber Issues at the State Department explained that the U.S. objected to the GGE due to the lack of international law restraints imposed on member States, inferring the application of force law as one of these).

15. Michele G. Markoff, Dept'y Coordinator for Cyber Issues, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017), https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ (explaining different aspects the GGE failed to address); *see also ICT Definition*, TECH TERMS, https://techterms.com/definition/ict (last visited Jan. 28, 2021).

lead to destabilization.[16] The main issue has been that, although most of the states involved in these meetings agree on the language of international law, they fundamentally disagree as to what that language means and whether or not it applies to cyber-attacks.[17]

A. *Typology: Cyber-attack, Cyber-warfare, & Cyber-crime Defined.*

There is currently no accepted consensus on the definition of "cyber-warfare" or "cyber-attack," and many groups use a variety of terminology and definitions.[18] As a general matter, however, "cyber-warfare" is often defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[19] Cyber-warfare is carried out by means of "cyber-attacks".[20] Two main definitions of "cyber-attack" are important for this paper: (1) the United States government's definition, and (2) the Shanghai Cooperation Organization's (SCO) definition.[21]

The U.S. government defines a "cyber-attack" as:

---

16. Markoff, *supra* note 15.

17. MOYNIHAN, *supra* note 13, at 53. For a more detailed description of the U.N. groups as well as regional State groups that are planning to meet in 2020 and 2021, *see id.* at 52–54.

18. Hathaway et al., *supra* note 4, at 823.

19. RICHARD CLARKE & ROBERT KNAKE, CYBERWAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (2010) (explaining in general the definition of "cyber-warfare").

20. *See* Steve Ranger, *What Is Cyberwar? Everything You Need to Know About the Frightening Future of Digital Conflict*, ZDNET (Dec. 4, 2018, 02:19), https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/ ("Cyberwarfare refers to the use of digital attacks – like computer viruses and hacking").

21. The SCO is self-defined as a counter-terrorism cooperation and intelligence sharing organization formed in 2001, composed of China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Uzbekistan, India, and Pakistan as member States. Iran, Afghanistan, Belarus, and Mongolia are "observer" States, meaning they are interested in becoming full members. *About SCO*, THE SHANGHAI COOPERATION ORG. (Jan. 9, 2017), http://eng.sectsco.org/about_sco/; Eleanor Albert, *The Shanghai Cooperation Organization*, COUNCIL OF FOREIGN REL., https://www.cfr.org/backgrounder/shanghai-cooperation-organization (last updated Oct. 14, 2015).

> A hostile act using a computer or related networks or systems, and *intended to disrupt and/or destroy an adversary's critical cyber systems*, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves – for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.[22]

By confining cyber-attacks to hostile acts specifically intended to disrupt or destroy critical cyber systems, this definition comes off as very narrow and mechanical. In contrast, the SCO broadly defines an "information war" as, in part, a "mass psychologic[al] brainwashing to destabilize society and state, as well as to force the state to take [*sic*] decisions in the interest of an opposing party."[23] Furthermore, the SCO considers the

---

22. Memorandum from Gen. James E. Cartwright for Chiefs of the Mil. Servs., Commanders of the Combatant Commands, and Directors of the Joint Staff Directories (Nov. 2010) (emphasis added); *see also* PRESIDENTIAL POLICY DIRECTIVE (PPD-20), *U.S. Cyber Operations Policy* 2 (Oct. 16, 2012), http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf (defining "malicious cyber activity" as "activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.").

23. The NATO Cooperative Cyber Defence Centre of Excellence, Unofficial Translation of AGREEMENT BETWEEN THE GOVERNMENTS OF THE MEMBER STATES OF THE SHANGHAI COOPERATION ORGANIZATION ON COOPERATION IN THE FIELD OF INTERNATIONAL INFORMATION SECURITY, 61ST PLENARY MEETING 209 (Dec. 2, 2008) https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf [hereinafter SCO Agreement Unofficial Translation]; *but see* Official Translation of AGREEMENT ON COOPERATION IN ENSURING INTERNATIONAL INFORMATION SECURITY BETWEEN THE MEMBER STATES OF THE SCO, 61ST PLENARY MEETING 9 (Dec. 2, 2008) http://eng.sectsco.org/load/207508/ [hereinafter SCO Agreement Official Translation] (translating this to "psychologically manipulating masses of the population to destabilize society and the State, and also forcing the state to take decisions in the interest of the opposing party" in the SCO official English-translated version).

spreading of information that is harmful to "social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states" to be one of the main threats to information security.[24] Thus, by focusing on attacks on social and political stability, the SCO definition seems to focus more on broad destabilization than just cyber system disruption like the U.S. definition.

This confined definition has negative implications on international humanitarian law.[25] By suggesting that harm to social, political, and economic systems might justify a government response, the SCO's definition runs the risk of allowing governments to suppress the political speech of dissenters by arguing that such dissent destabilizes society and the state.[26] While the First Amendment protects freedom of expression in the U.S., acceptance of the SCO's definition in countries without the same protections would create a serious human rights threat to citizens of those countries.[27] The U.S. definition of cyber-attack does not leave room for these types of expression restriction justifications because it is mainly focused on the protection of data and computer systems, and less on social and political impact.[28] This is the main reason it is imperative that changes to international law be made in favor of the U.S. definition rather than the SCO definition. The SCO's core membership includes countries with legal and regulatory regimes that tolerate (if not

24. SCO Agreement Unofficial Translation *supra* note 23, at 203; *but see* SCO Agreement Official Translation *supra* note 23, at 2 (translating this to "Dissemination of information prejudicial to the socio-political and socioeconomic systems, spiritual, moral and cultural environment of other States" in the SCO official English-translated version).

25. *See* Markoff, *supra* note 15 (discussing how omitting international humanitarian law from the GGE as it applies to State's use of Information Communications Technology sends a troubling signal).

26. Hathaway et al., *supra* note 4, at 825; Tom Gjelten, *Seeing the Internet as an "Information Weapon,"* NAT'L PUB. RADIO (Sept. 23, 2010, 2:00 AM), http://www.npr.org/templates/story/story.php?storyId=130052701.

27. *See* Gjelten, *supra* note 26 (discussing Chinese and Russian efforts to limit Internet communications among their citizens); U.S. CONST. amend. I.

28. *See* Memorandum from Gen. James E. Cartwright, *supra* note 22 (defining "cyber-attack" as a "hostile act using computer or related networks or systems and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions").

authorize or require) pervasive human rights abuses.[29] Thus, the SCO's definition may have even been designed with precisely this type of pre-planned justification in mind.[30] In June 2019, for example, China conducted a "denial of service" attack on Telegram, an encrypted messaging service that was being used by Hong Kong protestors, to disrupt their communications and coordination of the recent pro-free speech protests that have erupted in Hong Kong.[31]

Given the current lack of consensus on terminology and applicability of cyber-attacks to international law, the U.S. and SCO have been competing for their respective view to be adopted internationally. In 2011 and 2015, member states of the SCO submitted its *International Code of Conduct for Information Security* (the "Code") to the UN General Assembly.[32] The SCO claims this Code is intended "to push forward the international debate on international norms on information security, and help

29. *See* U.S. DEP'T OF STATE, 2018 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES: CHINA (INCLUDES TIBET, HONG KONG, AND MACAU) – CHINA 29, March 13, 2019, https://www.state.gov/wp-content/uploads/2019/03/CHINA-INCLUDES-TIBET-HONG-KONG-AND-MACAU-2018.pdf (discussing China's 2017 Cybersecurity Law, which broadly allows the government to "monitor, defend, and handle cyber security risks and threats originating from within the country or overseas sources, criminalizes using the internet to "creat[e] or disseminat[e] false information to disrupt the economic or social order," and codifies the authority of security agencies to cut communications networks across an entire geographic region during "major security incidents."). China has also permanently blocked international media outlets, such as the *New York Times*, as well as the websites of human rights organizations like Amnesty International and Human Rights Watch. *Id.* at 31. *See also* U.S. DEP'T OF STATE, 2017 COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES: RUSSIA 1 (Apr. 20, 2018), https://www.state.gov/wp-content/uploads/2019/01/Russia.pdf (listing the "blocking and filtering of internet content and use of cyberattacks to disrupt peaceful internet discussion" as one of the most significant human rights issues occurring in Russia).

30. Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 458–59 (2011) ("[M]ajor state actors in this area are likely to have different views on legal line drawing because they perceive a different set of strategic risks and opportunities.").

31. *Significant Cyber Incidents*, *supra* note 3.

32. Eneken Tikk & Mika Kerttunen, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, CYBER POL'Y INST. 19 (2017), https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf; Sarah McKune, *An Analysis of the International Code of Conduct for Information Security*, THE CITIZEN LAB (Sept. 28, 2015), https://citizenlab.ca/2015/09/international-code-of-conduct/.

forge an early consensus on this issue."[33] Critics of the Code, however, note that it raises serious human rights concerns because its language prioritizes state sovereignty and territorial dominance in cyberspace above all other concerns.[34] This language, along with the above-mentioned trends exhibited by the SCO, including its broad, means-based definition of "information warfare,"[35] indicates that its member countries would likely be able to legally violate human rights via the use of cyber-technology were this Code adopted internationally. Therefore, aside from simply protecting its own domestic interests, the U.S. also has an interest in promoting and protecting freedom of expression and association around the world.

In addition to the domestic human rights concerns, the SCO's positions also raise questions about how its member countries view cyber-attacks targeting foreign political elections. Specifically, could they justify election interference under the theory that certain foreign elections equate to the spreading of information that is harmful to "social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states?"[36] There is some indication they already are.[37] Several member states have a history of interfering, or attempting to interfere, with the elections of other countries with which they disagree either socially, politically, or economically.[38] For example, in July 2018, the U.S. Department of Justice (DOJ) indicted 12 Russian intelligence officers who were found to have

33. Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan, Letter dated Jan. 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the U.N. General Assembly addressed to the U.N. Secretary-General, U.N. Doc. A/69/273 (Jan. 13, 2015).

34. McKune, *supra* note 32.

35. Hathaway et al., *supra* note 4, at 825.

36. SCO Agreement Unofficial Translation *supra* note 23, at 203; *but see* SCO Agreement Official Translation *supra* note 23, at 2 (translating this to "Dissemination of information prejudicial to the socio-political and socioeconomic systems, spiritual, moral and cultural environment of other States" in the SCO official English-translated version).

37. *See generally Significant Cyber Incidents, supra* note 3 (documenting significant cyber incidents since 2006).

38. *See id.* (detailing examples of member states meddling with other countries' elections).

carried out large-scale cyber-attacks against the Democratic National Committee and Hillary Clinton's campaign just before the 2016 presidential election by targeting election infrastructure and local election officials.[39] Similarly, in February 2019, U.S. Cyber Command, a branch of the Department of Defense (DOD), announced that during the 2018 U.S. midterm elections a Russian company involved in information operations against the U.S. during the 2016 presidential election had tried to access election information.[40]

There has been no indication that similar attempts on U.S. electoral systems will dissipate in the near future. In fact, there are indications that China may be the next perpetrator.[41] Specifically, China's motives look very similar to Russia's in 2016 and 2018[42], and China has shown unique signs of a long-term scheme to weaken the United States and become what its leadership has called a "cyber superpower."[43] Thus, the importance of the U.S. leading conversations on changes in

---

39. *Id.*

40. *Id.* The U.S. is not always the target. For example, in March 2019, Russian state-sponsored hackers targeted several European government agencies just ahead of controversial European Union elections in May. *Id.* Also, in March 2019, Chinese and Russian state-sponsored hackers hacked into Indonesia's voter database prior to Indonesia's presidential and legislative elections. *Id.*

41. *See* Dustin Volz, *U.S. National Security Advisor Says China Targeting 2020 Election*, WALL STREET J., (Aug. 9, 2020, 5:17 PM), https://www.wsj.com/articles/u-s-national-security-adviser-says-china-targeting-2020-election-11597007831.

42. Russia's increased use of cyber-attacks has been occurring under the guise of three main objectives: (1) to gather intelligence that benefits Russia in the Ukraine-Syrian conflict, (2) to influence operations in support of their military and political goals, and (3) to continue to build their cyber-capabilities for future use. Similarly, China's motives include: (1) to gather intelligence that benefits China amidst escalating trade tensions with the U.S., (2) to influence operations in support of their military and political goals to become a world super power, and (3) to continue to build their cyber-capabilities for future use in order to become an economic leader and a cyber superpower. *See* James R. Clapper, Dir. of Nat'l Intelligence, Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community (Feb. 9, 2016); ASIA PACIFIC REGIONAL SECURITY ASSESSMENT 2019, *supra* note 11. *See generally* Xi Jinping, Report at the 19th National Congress of the Communist Party of China: Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era (Oct. 18, 2017).

43. Rogier Creemers et al., *Lexicon: 网络强国 Wǎngluò Qiángguó*, NEW AMERICA (May 31, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo.

international law as it relates to cyber-attacks is not only crucial for the international community in general but may be of use to the U.S. as these threats increase.[44]

Lastly, "cyber-crimes" are another form of cyber operations.[45] Cyber-crime also has no uniformly accepted definition but has certain characteristics that most countries seem to agree upon.[46] Cyber-crimes are generally recognized as computer-based illegal acts, violating either domestic or international criminal law, but unlike "cyber-attacks," most cyber-crimes involve non-state actors and do not have a political or national security purpose.[47] The most common examples in the U.S. and Europe include online piracy, distribution, and possession of child pornography, and common forms of hacking of personal data such as credit card information.[48] These types of cyber activities occur below the level of a "use of force," and have not been addressed in detail by international laws but rather are left mostly to individual states to legislate.[49] Thus, this paper will focus on cyber-warfare and cyber-attacks, rather than cyber-crimes.

---

44. *See, e.g.*, Abigail Ng, *China is the 'Most Serious Threat' to the United States, Says Former Security Advisor to Obama*, CNBC NEWS (Jan. 13, 2020, 12:46 AM), https://www.cnbc.com/2020/01/13/china-is-the-most-serious-threat-to-the-united-states-james-jones.html; Robert Burns & Matthew Lee, *US Defense Chief Slams China as Rising Threat to World Order*, ABC NEWS (Feb. 15, 2020, 9:30 AM), https://abcnews.go.com/International/wireStory/us-defense-chief-slams-china-rising-threat-world-69001913; Patricia Zengerle, *CIA Says China, Russia Pose Biggest Cyber Attack Threats to U.S.*, INS. J. (Jan. 30, 2019), https://www.insurancejournal.com/news/national/2019/01/30/516177.htm.

45. *See generally* Sylvia Kierkegaard, *International Cybercrime Convention, in* CYBER WARFARE AND CYBER TERRORISM 469, 470 (2007).

46. *Id.* (noting that one source defines it as any use of a computer as an instrument to further illegal ends) (internal quotations omitted).

47. Hathaway et al., *supra* note 4, at 834.

48. *See generally* H. MARSHALL JARRET ET AL., PROSECUTING COMPUTER CRIMES 102–03, 151 (U.S. Dep't of Justice, 2d. ed. 2010) (providing an overview of the prosecution of computer crimes). *See* Cyber Crime, FBI, http://www.fbi.gov/about-us/investigate/cyber (last visited Feb. 17, 2021); Convention of Cybercrime, Council of Europe, art. 9, Nov. 23, 2001, E.T.S. No. 185, (entered into force July 1, 2004) (establishing that parties to the Convention must adopt measures holding offenses related to child pornography as criminal offenses).

49. *See* INTERNATIONAL GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 18 (Michael N. Schmitt ed., 2013), http://csef.ru/media/articles/3990/3990.pdf [hereinafter TALLINN MANUAL 1.0].

B. *Cyber-attacks do not cleanly fit within pre-existing international legal frameworks for holding states responsible.*

Drawing the line between what is and is not a punishable offense in the cyber-attack context is made increasingly difficult by the existing law of war framework. Specifically, none of the drafters of these frameworks anticipated their application to cyber-attacks – a futuristic form of attack that has become a reality only in the last two decades.[50] In light of this rapidly emerging warfare, many states have been struggling over the answers to the following questions: (1) Can a cyber-attack ever legally amount to an act of war under international law, and (2) what options do states have for responding to such attacks?[51]

In general, there are two main categories of international law governing warfare between states: *jus ad bellum* and *jus in bello*.[52] *Jus ad bellum* refers to the law that governs when states may resort to war or to the use of armed force generally, whereas *jus in bello* refers to the law governing the conduct of parties that are already engaged in an armed conflict.[53] This paper will focus only on *jus ad bellum*. This set of laws prohibits "use of force" (including threats of using such force), "armed attacks", "threats to the peace," "breach of the peace," and "acts of aggression."[54] To date, the most important source of *jus ad bellum* is the U.N.

---

50. *See* Hathaway et al., *supra* note 4, at 817, 840 (explaining that cyberattacks are relatively new and therefore the drafters of legal frameworks were unable to predict them).

51. *See The Application of International Law in Cyberspace: State of Play* , UNITED NATIONS (Oct. 25, 2018) https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/ (summarizing the Meeting Minutes from a panel discussion hosted by the UN and EU, in which the panel discussed whether international law applies to cyberspace and what responses States should consider).

52. RICHARD P. DIMEGLIO ET AL., LAW OF ARMED CONFLICT DESKBOOK 8 (William J. Johnson & Andrew D. Gillman eds., 2012), http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf.

53. *What Are Jus Ad Bellum and Jus In Bello?*, INT'L COMM. OF THE RED CROSS (ICRC) (Jan. 22, 2015), https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0.

54. NILS MELZER, UNIDIR RESOURCES, CYBERWARFARE AND INTERNATIONAL LAW 6 (2011), https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Charter.[55] Other aspects of *jus ad bellum* are derived from customary law and its accompanying international jurisprudence, and thus will be discussed separately.[56] They all, however, seem to pose their own problems in the context of cyber-attacks.

1. *The U.N. Charter*

Article 2(4) of the U.N. Charter provides that member states must "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[57] Although some have argued that Article 2(4) provides a broad prohibition on force, including acts like economic and political coercion,[58] the overwhelming majority of commentators today consider "force" in Article 2(4) to be synonymous with "armed force."[59] However, the International Court of Justice (ICJ) has stated that the prohibition on the use of "force" applies to "any use of force, regardless of the weapons employed."[60] To date, no state has ever formally argued that a cyber-attack is a prohibited "use of force" per Article 2(4).[61] However, the increase in cyber-attacks in recent years increases the likelihood that states may at some point begin

55. *Id.*

56. *Id.*

57. U.N. Charter art. 2, ¶ 4. There are also two exceptions to this rule: (1) actions taken as part of collective security operations, and (2) actions taken in self-defense. *See* U.N. Charter art. 39, 51 (stating in Article 39 that the security council will make recommendations or decide measures to be taken against "any threat to the peace, breach of the peace, or act of aggression", and in Article 51 that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence").

58. *See, e.g.*, Comment, *The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations*, 122 U. PA. L. REV. 983, 988 (1974).

59. *See e.g.*, Daniel Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, *in* 76 INT'L L. STUDIES: COMPUTER ATTACK & INT'L L. 73, 80–82 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002); Albrecht Randelzhofer, *Article 2(4)*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 117, (Bruno Simma ed., 2002); Marco Roscini, *World Wide Warfare–Jus ad Bellum and the Use of Cyber Force*, *in* 14 MAX PLANCK Y.B. U.N. L. 85, 105 (2010).

60. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

61. Hathaway et al., *supra* note 4, at 840.

to respond to cyber-attacks with conventional military means if no international framework governing cyber-attacks is agreed upon.[62]

There are only two generally agreed upon exceptions to Article 2(4)'s prohibition of the threat or use of force: (1) actions authorized by the U.N. Security Council under Chapter VII of the U.N. Charter, and (2) actions that constitute "self-defense" under Article 51.[63] Under Chapter VII, the U.N. Security Council can label threats or uses of force as illegal and then may choose the appropriate response measure.[64] Chapter VII gives the Council three options for courses of action in response to an illegal threat or use of force: (1) Article 39, (2) Article 41, and (3) Article 42.[65] With regard to Articles 39 and 41, the Council's decision is expected to be grounded in an intention to restore international peace and security.[66] Article 39 allows the Council make a non-binding, permissive authorization (military or non-military).[67] Article 41 provides a list of binding, non-military enforcement measures, including the interruption of railroad, sea, air, postal, telegraphic, radio, and other communications, as well as the severance of diplomatic relations.[68] Notable for the cyber-attack context, Article 41 specifically refers to an "interruption of . . . communication" as a "measure *not* involving armed force."[69]

Lastly, Article 42 allows the Council to authorize military action pursuant to a special agreement made between U.N. member states.[70] As long as the U.N. Security Council has not yet acted under one of these articles, Article 51 allows states to use

62. *See* U.S. DEP'T OF DEFENSE, CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO SECTION 934 OF THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, at 2 (2011) (declaring that the United States reserves the right to respond to cyber-attacks using "all necessary means – diplomatic, informational, military, and economic").

63. DIMEGLIO ET AL., *supra* note 52, at 31.

64. *Id.* at 32.

65. *Id.*

66. *Id.*

67. *Id.*; U.N. Charter, art. 39.

68. DIMEGLIO ET AL., *supra* note 52, at 32–33; U.N. Charter art. 41.

69. U.N. Charter art. 41 (emphasis added).

70. U.N. Charter art. 42.; DIMEGLIO ET AL., *supra* note 52, at 33.

self-defense in the event of an "armed attack."[71] The ICJ has defined "armed attack" as "the most grave form of the use of force."[72] This language, which will be discussed further later, is not always easily applied in the cyber-attack context, given its implicit focus on physical force through the use of weapons.

Additionally, as will be discussed later, even if these definitions could be molded to fit the characteristics of cyber-attacks, an inherent issue may still linger: attribution. Article 2(4) is only addressed to states and prohibits their threat or use of force in their "international relations" with other states.[73] Thus, practically-speaking, states must be able to legally attribute which other state threatened or used force against them. This requires the actions to be "performed by persons or entities acting on behalf or with the authorization or endorsement of a state so as to engage its international legal responsibility for their behaviour."[74] The issues posed by this come to light in two scenarios in the cyber-attack context: (1) when the state-actor hides his/her identity or his/her ties to a state, and (2) when the attacker is a non-state actor.[75] As mentioned, attribution can be especially difficult in the cyber-context. Additionally, because the use of force by anyone other than a legally attributable state actor is not covered by the U.N. Charter, a state under attack by a non-state actor would need to look to another area of international law.

Thus, the two main issues with the U.N. Charter as applied to cyber-attacks are (1) its specific language and (2) attribution.

---

71. U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.").

72. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 191 (June 27).

73. According to Article 4 of the U.N. Charter, only States can be "members" of the United Nations as referred to in Article 2(4). U.N. Charter art. 4, ¶ 1.

74. MELZER, *supra* note 54, at 10.

75. *See* Waxman, *supra* note 30, at 444 (discussing how forensics necessary to identify a cyber-attacker is very difficult and may not be possible); Sico van der Meer, *How States Could Respond to Non-State Cyber-Attackers*, CLIGENDAEL (June 2020), https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf (arguing states may utilize non-state actors in cyber-attacks to circumvent attribution and thus consequences).

But even if cyber-attacks cannot work under the U.N. Charter, another potential set of international laws that may be applicable to cyber-attacks are those that enforce the principle of state responsibility. These laws allow the U.N. to hold accountable states which are found to have committed internationally wrongful acts.

2. *Laws enforcing the principle of state responsibility for internationally wrongful acts: sovereignty, non-intervention, and due diligence.*

The other body of law that could be used to fight cyber-attacks is known as "state responsibility."[76] Under this set of international laws, a state can be held responsible for an "internationally wrongful act" if it (1) is classified as a breach of an international obligation of the state and (2) is attributable to the state under international law.[77] As to the first element–a breach of an international obligation of the state–there are a number of international obligations that states are under. There are three main types of international legal obligations that might be breached through a cyber-attack: (a) sovereignty, (b) the duty of non-intervention, and (c) the duty of due diligence.[78] First, breaches of sovereignty involve an infringement on a state's territorial integrity, which is generally interpreted as physical territorial integrity.[79] Similar to the U.N. Charter's "armed force" element, this can cause issues in the cyber-attack context.

---

76. *See* G.A. Res. 56/83 (Dec. 12, 2001) (annexing the Articles on State Responsibility to a U.N. resolution).

77. *Id.* art. 2.

78. Barrie Sander, *Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections*, 18 CHINESE J. INT'L L. 1, 17–18 (2019). *But cf.* Dan Efrony & Yuval Shany, *A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 591–92 (2018) (discussing how officials in the United States and United Kingdom contested sovereignty as international legal "principle" rather than a "rule" (obligation), despite the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* treating sovereignty as a primary rule of international law).

79. INT'L GRPS. OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 20 (Michael N. Schmitt, ed., 2017) [hereinafter TALLINN MANUAL 2.0].

Second, principals of non-intervention are applied through a two-part rule. The ICJ has stated that an act breaches international law under non-intervention principles if: (1) the act is "bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely" and (2) the act uses "methods of coercion."[80] The precise scope of "coercion," as used by the ICJ here, is disputed. Some argue coercion should be defined broadly as including almost any type of state manipulation for self-serving purposes, including economic or political coercion.[81] The U.N. General Assembly has taken a similarly broad view of "coercion" in the past, stating that no state possesses "the right to intervene, directly or indirectly, for any reason whatever, in sovereignty of any other State" or use "any . . . measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights."[82] Others argue coercion should be narrowly defined as physically forcing a state to do something.[83] As will be discussed, which view of coercion is applied affects the degree to which the doctrine can be applied to cyber-attacks.

Third, the ICJ held a state must not "allow knowingly its territory to be used for acts contrary to the rights of other states" and thus has a duty of due diligence in protecting other state from known threats within its territory.[84] Applied to the cyber-attack context, the duty of due diligence consists of three main elements: (1) "knowledge" of a cyber operation being carried out from within its territory, (2) a failure to undertake "all reasonably available measures" to end this cyber operation, and (3) the cyber operation is "contrary to the rights" of, and produces "serious adverse consequences for other states."[85] As will be discussed, these requirements also may not fully apply in the cyber-context due to

80. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

81. *See* Derek W. Bowett, *International Law and Economic Coercion*, 16 VA. J. INT'L L. 245, 246 (1976).

82. G.A. Res. 2131 (XX) (Dec. 21, 1965); G.A. Res. 2625 (XXV) (Oct. 24, 1970).

83. *See* TALLINN MANUAL 2.0, *supra* note 79, at 317 (defining coercion as acts "designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way.").

84. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (April 9).

85. TALLINN MANUAL 2.0, *supra* note 79, at 43.

the inconspicuous nature of cyber-attacks and the resources it takes to combat large-scale attacks.

On their face, neither the U.N. Charter nor the law of state responsibility seems to clearly apply to the cyber-context given the patent differences between the nature of traditional warfare and cyber warfare. These differences, and the required modifications, will be discussed in detail later. First, however, it is necessary that the different types of cyber-attacks be clearly defined, as some of the suggested modifications would only be necessary for certain types of attacks, but not others.

C. *Types of cyber-attacks.*

Attackers use a variety of strategies when executing a cyber-attack (depending on their goal). Broadly, the two main techniques are cyber-tampering operations and cyber-influencing operations.[86] Cyber-tampering, or hacking, involves "disrupting, destroying, or altering computer systems or information resident in them."[87] On the other hand, cyber-influencing involves "the deployment of resources to alter the behaviour of a targeted audience."[88] There are several different types of cyber-influencing operations, including doxing and information operations.[89] Doxing involves the "exfiltration and leaking of non-public information."[90] Information operations involve the "deliberate use of newly-created or publicly available information to threaten, confuse, or mislead a target audience."[91] Examples of information operations include "trolling" and "fake news."[92] Large-scale cyber-

86. *See* Sander, *supra* note 78, at 4.

87. *Id.*; *see also* CHRIS TENOVE ET AL., DIGITAL THREATS TO DEMOCRATIC ELECTIONS: HOW FOREIGN ACTORS USE DIGITAL TECHNIQUES TO UNDERMINE DEMOCRACY 12 (2018) (categorizing these as cyber-attacks on systems and databases).

88. Sander, *supra* note 78, at 4; *see also* TENOVE ET AL., *supra* note 87, at 16–18 (categorizing these cyber-attacks as digital misinformation campaigns).

89. Sander, *supra* note 78, at 4.

90. *Id.*

91. *Id.*

92. *Id.* at 11; *see also* TENOVE ET AL., *supra* note 87, at 16–25 (examining the techniques that constitute both "trolling" and "fake news" and giving examples of both).

attack operations often use a combination of these strategies to accomplish their goals.[93]

1. *Cyber-tampering: hacking.*

Cyber tampering, commonly known as "hacking," is the more familiar form of cyber-attack.[94] Cyber tampering usually includes tricking people into providing account information and passwords, or downloading malware that infects their computer, such as through phishing e-mails that contain malware-ridden hyperlinks.[95] Hacking focused on influencing political elections can occur in the form of breaches of voting machines, voter lists, or other systems related to the election process, such as those that contain campaign information.[96]

There is significant evidence that foreign actors have attempted to hack U.S. voting systems in the past.[97] In July 2018, for example, a U.S. Senator's re-election campaign was unsuccessfully targeted by hackers affiliated with Russia's intelligence agency by sending phishing emails to staffers in her office in attempts to steal passwords and access sensitive information related to the campaign.[98] On an even larger scale, in February 2018 the Department of Homeland Security confirmed that Russian hackers had successfully hacked into voter registration lists in several U.S. states prior to the 2016 presidential election.[99] Even if election-related citizen information is being legally obtained, such as through an authorized data collection by the government (i.e., law-enforcement systems) or a corporation (i.e., credit card and banking companies), this information can nonetheless be hacked

93. TENOVE ET AL., *supra* note 87, at 12.

94. *Id.*

95. *Id.* at 12–13; *see also* Liam Tung, *Google: Our Hunt for Hackers Reveals Phishing is Far Deadlier than Data Breaches*, ZDNET (Nov. 10, 2017, 12:19 PM), https://www.zdnet.com/article/google-our-hunt-for-hackers-reveals-phishing-is-far-deadlier-than-data-breaches (discussing studies showing that simple trickery through phishing tends to cause more damage than direct hacking of information).

96. TENOVE ET AL., *supra* note 87, at 13.

97. *Id.*

98. *Significant Cyber Incidents*, *supra* note 3.

99. *Id.*

from these lawful possessors.[100] While cyber-tampering has been the traditional strategy utilized by cyber-attackers since the inception of cyber-warfare, the use of cyber-influencing has become increasingly prevalent as social media has become more popular and thus, more easily manipulated by attackers.[101]

2. *Cyber-influencing: doxing and information operations.*

Cyber-influencing includes "doxing," and information operations.[102] "Doxing" occurs when a hacker infiltrates a computer system in order to leak non-public information.[103] In the political context, the purpose of doxing is to influence peoples' reputations and alter the outcomes of elections as a result.[104] Doxing can take shape in two forms: traditional whistleblowing (exposing wrongdoing to promote the public good), or strategic hacks (leaking of material that is in the interest of the hacker, but not necessarily in the interest of the public).[105] The June 2013 leaks by Edward Snowden, a former systems administrator with the National Security Agency (NSA), revealing documents showing evidence of cyber-espionage conducted by the U.S. against Chinese targets, is an example of traditional

100. *See* Nils Gilman, Jesse Goldhammer, & Steven Weber, *Can You Secure an Iron Cage?*, LIMN, https://limn.it/can-you-secure-an-iron-cage/ (last visited Feb. 5, 2021) (discussing the hack of private consulting firms which had contracted with the U.S. government to conduct background checks on employees).

101. *See, e.g.*, *The Rise and Rise of Fake News*, BBC NEWS (Nov. 6, 2016), https://www.bbc.com/news/blogs-trending-37846860; *see also* Michael Barthel et al., *Many Americans Believe Fake News is Sowing Confusion*, PEW RSCH. CTR. (Dec. 15, 2016), https://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/ (discussing the belief held by a majority of Americans that fake news is increasingly prevalent).

102. Sander, *supra* note 78, at 4.

103. *Id.*

104. *See, e.g.*, E. Gabriella Coleman, *The Public Interest Hack*, LIMN, http://limn.it/the-public-interest-hack/ (last visited Feb. 5, 2021) (discussing a doxing feud between a white supremacist radio host and anonymous 4chan users, as well as similar incident in which someone hacked Sarah Palin's email and posted what they found online in an attempt to damage her reputation ahead of the 2008 presidential election); *see also Significant Cyber Incidents*, *supra* note 3 (discussing the July 2018 incident in which Russian intelligence officers were indicted by the U.S. Department of Justice (DOJ) for stealing and leaking confidential emails from the Democratic National Committee and the Hillary Clinton campaign).

105. Sander, *supra* note 78, at 8–9; *see also* TENOVE ET AL., *supra* note 87, at 13–14.

whistleblowing, with someone from the "inside" exposing information with intentions to benefit the public.[106] The leaking of Democratic National Committee and Clinton campaign emails prior to the 2016 presidential election by Russian hackers is an example of a strategic hack.[107] In the author's opinion, strategic hacking is the more dangerous of the two types of doxing because the information leaked is more likely to be "tainted," meaning doctored or wholly fake.[108] Because election interference is almost never done with the public good in mind, it falls squarely under strategic hacking.

Cyber-influencing also includes "trolling" and what is commonly called "fake news," collectively called "information operations."[109] Trolling involves attackers causing disruption, or triggering or exacerbating conflict on the internet.[110] Trolls often use threats of doxing and intimidation, including threats of death, sexual assault, harm to one's family, or reputational damage, and often target journalists, political dissenters, and members of

106. *See Significant Cyber Incidents*, *supra* note 3. Although the platform "Wikileaks" might be confused as a form of traditional whistleblowing, Wikileaks is often used as a platform for strategic hackers to dump leaked material anonymously. *See, e.g.*, *id.* (discussing when the Department of Homeland Security identified Russia as responsible for the 2016 DNC email hacking and acknowledging that Russia then use Wikileaks to disseminate the emails obtained in the hack); *see also* Ethan Lozano et al., *Wikileaks & Whistleblowing: Digital Information Leakage and Its Impact on Society*, STANFORD UNIV., https://cs.stanford.edu/people/eroberts/courses/cs181/projects/2010-11/WikiLeaks/online.html (last visited Feb. 5, 2021) (discussing the differences between traditional offline leaks and online leaks through websites like WikiLeaks).

107. "Strategic hacking" is not to be confused with cyber-tampering ("hacking"). Strategic hacking is simply the name of a type of cyber-influencing. *See* Sander, *supra* note 78, at 9 (classifying "strategic hacking" as a subset of "doxing," itself a type of cyber-influencing).

108. TENOVE ET AL., *supra* note 87, at 14; *see also* Adam Hulcoop et al., *Tainted Leaks: Disinformation and Phishing With a Russian Nexus*, THE CITIZEN LAB (May 25, 2017), https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/ (defining tainted leaking as the "deliberate seeding of false information within a larger set of authentically stolen data").

109. Sander, *supra* note 78, at 10–11.

110. *See* TENOVE ET AL., *supra* note 87, at 22–23 (including "[u]ncivil, threatening and disruptive behaviours online," and "a specific kind of political activity that is marked by a refusal to participate in the kind of productive exchange of ideas that marks democratic politics" as alternate definitions as well).

opposition parties.[111] states can utilize this strategy on its own citizens as well as on citizens of a target country.[112] For example, China recently exhibited this type of behavior when its government reportedly intimidated and threatened Chinese protesters online and in the media.[113] In addition to threats, memes[114] can be used as a form of more subtle trolling. Specifically, attackers can use them to inflame political and cultural polarization by disseminating extreme viewpoints, while simultaneously downplaying their dangerous effects under a guise of light-hearted joking on the internet.[115] Memes can specifically favor one candidate or party over the other, or can simply act as a tool for creating division within a party or country.[116] In October 2019, for example, Mark Zuckerberg, the owner of Facebook, announced that the company had recently caught Russian and Iranian backed hackers creating fake accounts, mostly on Instagram, and sharing original meme

---

111. *See generally* Samantha Bradshaw & Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation* 9–11, (Univ. of Oxford Computational Propaganda Rsch. Project, Working Paper No. 2017.12, 2017), http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf (discussing state-sponsored trolling operations across 28 countries). *See, e.g.*, Ken Dilanian, *Russian Trolls Who Interfered in 2016 U.S. Election Also Made Ad Money, Report Says*, NBC NEWS (June 5, 2019, 5:00 AM CDT), https://www.nbcnews.com/politics/national-security/russian-trolls-who-interfered-2016-u-s-election-also-made-n1013811 (discussing a Russian intelligence operation designed to undermine American democracy and hurt Hillary Clinton).

112. *See, e.g.*, Lily Kuo, *Beijing's New Weapon to Muffle Hong-Kong Protests: Fake News*, THE GUARDIAN (Aug. 11, 2019, 5:00 AM), https://www.theguardian.com/world/2019/aug/11/hong-kong-china-unrest-beijing-media-response; Donie O'Sullivan, *After FBI Tip, Facebook Says It Uncovered Russian Meddling*, CNN (Sept. 1, 2020, 10:22 PM ET), https://www.cnn.com/2020/09/01/tech/russian-troll-group-facebook-campaign/index.html.

113. Kuo, *supra* note 112.

114. TENOVE ET AL., *supra* note 87, at 17.

115. *See id.* at 17, 23–24.

116. *See* Andrew Hutchinson, *Facebook Implements New Rules on the Use of Memes by Political Candidates*, SOC. MEDIA TODAY (Feb. 15, 2020), https://www.socialmediatoday.com/news/facebook-implements-new-rules-on-the-use-of-memes-by-political-candidates/572381/; Matthew Rosenberg, Nicole Perlroth, & David E. Sanger, *'Chaos Is the Point': Russian Hackers and Trolls Grow Stealthier in 2020*, N.Y. TIMES (Jan. 10, 2020), https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html.

content.[117] Some of the memes were designed to generally create divisiveness between the Democratic party, and some to specifically promote the re-election of Donald Trump.[118] Zuckerberg also stated that China had made attempts to influence operations via Facebook, but that Facebook's security team had been able to step in before much was seen by users.[119] In contrast, the Russian and Iranian efforts reached large audiences before being detected.[120]

Cyber-influencing also includes the spread of misinformation, more commonly known as "fake news."[121] Although election experts have long worried about the electoral effects of the uninformed voter, cyber influencing tactics like fake news has increased the number of potentially *misinformed* voters.[122] This category, much like trolling, often uses fake social media accounts, memes, and other organic forms of disinformation spread by users.[123] The type of medium used is very important to the effectiveness of fake news. Specifically, the amount of influence a piece of misinformation has can also be artificially expanded through the use of algorithms, automation, and "targeting."[124] These strategies allow the attacker to hone in their message to certain groups of people and to spread the information in strategic ways.[125] "Bots," for example, can be used to suppress

117. Jason Abbruzzese, *Mark Zuckerberg: Facebook Caught Russia and Iran Trying to Interfere in 2020*, NBC NEWS (Oct. 21, 2019, 11:53 AM CDT), https://www.nbcnews.com/tech/tech-news/mark-zuckerberg-facebook-caught-russia-iran-trying-interfere-2020-n1069366; Julia Carrie Wong, *Facebook Discloses Operations by Russia and Iran to Meddle in 2020 Election*, THE GUARDIAN (Oct. 21, 2019, 15.50 EDT), https://www.theguardian.com/technology/2019/oct/21/facebook-us-2020-elections-foreign-interference-russia.

118. Wong, *supra* note 117.

119. *Id.*

120. *Id.*

121. Sander, *supra* note 78, at 11.

122. TENOVE ET AL., *supra* note 87, at 16.

123. *Id.*

124. *Id.* at 17.

125. Samuel C. Woolley & Philip N. Howard, *Computational Propaganda Worldwide: Executive Summary* 4 (Univ. of Oxford: Project on Computational Propaganda, Working Paper No. 2017.11, 2017), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies ExecutiveSummary.pdf; *see also* Jonathan Albright, *Who Hacked the Election? Ad Tech Did. Through "Fake News," Identity*

already popular content that they do not want to spread, or to amplify content that attackers want to make seem more popular (which to make things even more difficult to track, can make things *actually* more popular).[126] Similarly, "sock puppets," which are fake accounts run by humans that enable attackers to spread information behind a hidden or misrepresented identity, can be used to make certain information seem more authentic by impersonating trusted sources.[127]

Because of the intangible, untraceable, and overall immeasurable nature of cyber-attacks, the use of these cyber-tampering and cyber-influencing tactics by foreign actors is not punishable under the laws as written. Therefore, I suggest that certain modifications be made to the language of these international laws in order to make them more applicable to cyber-attacks, specially to the tactics used to influence elections.

II. ANALYSIS

A. *Amendments that need to be made to the pre-existing legal frameworks in order to be applicable to cyber-attacks.*

Due to the lack of foresight regarding cyber-attacks at the time the pre-existing international law was drafted, it is no surprise that none of them fully encompass the attributes of cyber-attacks and cyber-warfare. However, there are a few changes that can be made to these laws that would make them more applicable to cyber-attacks.

1. *Modifying "armed force" to include the U.S. definition of*

Resolution and Hyper-Personalization, TOW CTR. (July 30, 2017), https://medium.com/tow-center/who-hacked-the-election-43d4019f705f (concluding that behavioral targeting strategies and identity technologies "are as sophisticated as it gets").

126. Alessandro Bessi & Emilio Ferrara, *Social Bots Distort the 2016 U.S. Presidential Election Online Discussion*, 21 FIRST MONDAY 11 (Nov. 7, 2016), https://firstmonday.org/ojs/index.php/fm/article/view/7090/5653.

127. TENOVE ET AL., *supra* note 87, at 17; *see, e.g.*, Ben Collins, Kevin Poulsen, & Spencer Ackerman, *Exclusive: Russians Impersonated Real American Muslims to Stir Chaos on Facebook and Instagram*, THE DAILY BEAST (Sept. 27, 2017, 4:29 PM ET), http://www.thedailybeast.com/exclusive-russians-impersonated-real-american-muslims-to-stir-chaos-on-facebook-and-instagram (describing a Russian linked imposter account impersonating a real organization).

cyber-attack would encompass cyber-tampering that doesn't result in physical consequences.

To recap, Article 2(4) of the U.N. Charter provides a very broad definition of "use of force."[128] However, the international community consensus seems to be that this simply means "armed force."[129] The ICJ has defined "armed attack" as "the most grave forms of the use of force."[130] This language seems clearly geared towards physical consequences. In light of this, there is an argument to be made that cyber-attacks amounting to physical destruction, death, and injury would fall under Article 2(4). For example, hacking into nuclear plant systems to cause a meltdown, hacking into a dam's controls and flooding a nearby populated area, or hacking into an airport's air traffic control system and disabling communications would all certainly result in physical consequences and could be punishable under Article 2(4) of the U.N. Charter.

This covers many forms of cyber-tampering, but what about the cyber-tampering that doesn't create physical destruction? Finding a way to fit these types of cyber-attacks under Article 2(4) is much more challenging. The ICJ later stated that the prohibition on the use of "force" applies to "any use of force, regardless of the weapons employed."[131] This indicates that Article 2(4) could apply to even those cases of cyber-attacks without physical consequences. But Article 41 weakens this argument, as it specifically refers to "interruption of . . . communication" as "measures *not* involving the use of armed force."[132] The context of Article 41, however, illustrates that this statement refers to state *responses* to an "armed attack,"[133] and not to the original attack itself. Thus, perhaps the aggressive

128. U.N. Charter art. 2, ¶ 4.

129. Hathaway et al., *supra* note 4, at 842.

130. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 101, ¶ 191 (June 27).

131. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244, ¶ 39 (July 8).

132. U.N. Charter art. 41 (emphasis added).

133. *See generally id.* (giving the authority to call on Member States to apply measures as a State response to threats to peace and acts of aggression).

intent of a cyber-attack would be enough to classify it as an "armed attack" under Article 2(4), arguing that cyber-tampering and cyber-influencing are technological "weapons."

But is there any indication that the international community sees it this way? Contrary to the widely accepted view that a state can use force in self-defense only in response to an "armed attack" – the gravest form of force – the U.S. has historically maintained that force can be used in self-defense in response to *any* amount of force used against it.[134] This comports with the ICJ's broad assertion that the prohibition on the use of "force" applies to "any use of force, regardless of the weapons employed."[135] Thus, the easiest way to make Article 2(4) more applicable to all cyber-tampering is to formally broaden the definitions of "use of force" and "armed attack." One way to do this would be to include a specific provision that ties in the United States' definition of cyber-attack. For example, "use of force" and "armed attack" could both be defined to include "[a] hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions."[136] With this modification, "force" and "armed" could be extended to apply not just to traditional weaponry, but also cyber-weaponry like that used for cyber-tampering.

However, even these broader definitions probably fail to cover cyber-influencing because cyber-influencing is usually much more subtle and leaves much less tangible evidence behind.[137] Due to the difficulties of reconciling a "use of force" or "armed attack" with things like trolling, doxing, and spreading fake news, cyber-influencing would likely best be addressed in a separate body of law. Adding it to Article 2(4) of the U.N. Charter most likely would risk over broadening the article and rendering it obsolete as a result. Instead, cyber-influencing could be addressed as an

134. Ryan Goodman, Cyber Operations and the U.S. Definition of "Armed Attack," Just Security (Mar. 8, 2018), https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack/.

135. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244, ¶ 39 (July 8).

136. Memorandum from Gen. James E. Cartwright, *supra* note 22, at 5.

137. *See* Sander, *supra* note 78, at 26–27 (explaining the complexity of attribution for cyber operations).

internationally wrongful act under the principle of state responsibility, which is already a much broader and more flexible framework of laws. However, each principle would also need slight modification in order to apply.

But even if Article 2(4) could be modified to include all cyber-tampering, the second incompatibility between cyber-attacks and the U.N. Charter is the issue of attribution. This issue is present in both the cyber-tampering and cyber-influencing contexts. With cyber-attacks, attribution can be difficult because it is almost always conducted remotely or behind technological disguises such as proxies and Virtual Private Networks (VPNs), which effectively scramble your location if anyone attempts to track the network connection.[138] Attackers also often utilize multiple computer systems in different states[139] or use anti-attribution technology that hides their identity or location.[140] Many cyber-attackers are also sophisticated non-state actors, either acting independently or as a cyber proxy for a state.[141] Additionally, because the person actually conducting the cyber-operations may not be clearly linked to the state, this can make it very difficult for victim states to provide a legal nexus between the breach of international law and said state, which is required for any action to be taken.[142] However, even if a specific state could be identified as being responsible for the cyber-attack, public acknowledgement of this attribution may not be desirable for the victim state for national security, public morale, and diplomacy purposes.[143] These attribution issues, inherent in the cyber-world,

---

138. *See* Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCI. AM. (June 11, 2011), https://www.scientificamerican.com/article/tracking-cyber-hackers/.

139. Sander, *supra* note 78, at 27.

140. Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. OF CONFLICT & SEC. L. 229, 234 (2012).

141. Luke Chircop, *A Due Diligence Standard of Attribution in Cyberspace*, 67 INT'L & COMP. L. Q. 643, 647 (2018); Hathaway et al., *supra* note 4, at 843 ("[S]tates generally do not engage in cyber-attacks openly, but rather try to hide their responsibility by camouflaging attacks through technical means and by perpetrating the attacks through non-state actors with ambiguous relationships to state agencies.").

142. Hathaway et al., *supra* note 4, at 843; Sander, *supra* note 78, at 27.

143. *See* Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 176–77 (2017).

may simply be unavoidable. In addition to being an obstacle to applicability under the U.N. Charter, this issue of attribution also comes up under the laws of state responsibility. These laws, discussed next, allow the U.N. to hold accountable states which are found to have committed internationally wrongful acts.

2. *Modifying the laws of state responsibility to better address cyber-tampering and cyber-influencing.*

i. *Sovereignty should be modified to encompass digital territory as well as physical.*

Breaches of sovereignty involve infringement of a state's territorial integrity, which is generally interpreted as physical territorial integrity.[144] This requirement poses a few issues in the cyber-context. First, cyber-attacks often cannot be said to result in "physical damage or injury" to a state.[145] However, unlike the U.N. Charter, it could be argued that breaches of sovereignty may actually reach farther than just "physical damage or injury." In the early stages of the digital age, experts almost unanimously asserted that attacks on cyber-space could not result in breaches of sovereignty because sovereignty rights protected strictly physical parameters.[146] However, most countries have, in practice, considered cyber-space to be legally tied to their "territory."[147] For example, states exercise this territorial sovereignty over cyberspace when they pass domestic cyber-crime laws.[148] One way to reconcile these views is the fact that cyber-

144. TALLINN MANUAL 2.0, *supra* note 79, at 20.

145. Duncan Hollis, *The Influence of War; The War for Influence*, 32 TEMPLE INT'L & COMP. L. J. 31, 42 (2018) ("[T]here is little precedent for treating the purely cognitive effects to which [influence operations] ultimately aspire as breaching sovereignty.").

146. *Id.*; David Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996).

147. *See* U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98 (July 22, 2015) (suggesting ways to protect the territory of the states from harmful acts in cyberspace) [hereinafter "GGE Report"].

148. *Id.* ¶ 13; *see, e.g.*, Julian Borger, *Brazilian President: US Surveillance a 'Breach of International Law*, THE GUARDIAN (Sept. 24, 2013, 12:27 PM), http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance (discussing the Brazilian President's rebuke against the reports of U.S. cyber-

space actually requires physical components within a state's territory to function, such as fiber-optic cables, copper wires, microwave relay towers, satellite transponders, and internet routers.[149] Thus, to address the physical territory element, the simplest fix would be to codify this practice into the text of the Articles on State Responsibility. For clarity, the updated articles should state that "territory" includes not only physical boundaries and possessions (which would cover cyber-tampering), but also violations of infrastructure sovereignty through technological means (to cover cyber-influencing). Specifically, it should state that sovereignty can be violated by an attempt to influence political and economic outcomes through the hostile use of computer or network systems. This should address the physical boundary obstacle in the current language. To address the physical damage element, the Articles would also need to broadly define damage or injury to the state. Damage should be defined as including compromised data (to cover cyber-tampering) and as damage or injury to the sovereign integrity of the state (to cover cyber-influencing). Although this can seem intangible, one way to measure damage from cyber-influencing is to measure the extent of audience reach. This makes sense because the state's injury grows with each person that is affected by doxing, that experiences trolling, or views fake news. This would cover both cyber-tampering efforts and cyber-influencing efforts by states without making the principle overly broad. However, extending the principle of sovereignty to attacks on the sovereign integrity of a state may necessarily overlap with non-intervention. Thus, changes to both may not be necessary to achieve a set of laws applicable to both cyber-tampering and cyber-influencing, but it's

---

espionage being committed against Brazil in the Edward Snowden leaks, and quoting her explicit condemnation of such actions as a breach of sovereignty). However, it should be noted that other countries that spoke out against these NSA leaks did not explicitly invoke sovereignty as a ground and thus it should not be assumed that cyber-attacks are universally considered breaches of territorial sovereignty. Russell Buchan, *The International Legal Regulation of State-Sponsored Cyber Espionage, in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES 65, 72 (Anna-Maria Osula and Henry Rõigas eds., 2016). Notably, China also spoke out generally against the reports about U.S. cyber-meddling but is a known perpetrator of cyber-meddling themselves. *Id.*

149. Patrick W. Franzese, *Sovereignty in Cyberspace: Can it Exist?*, 64 AIR FORCE L. REV., no. 1, 2009, at 1, 12.

important to discuss their individual weaknesses nonetheless because they may be applicable in different scenarios.

ii. *Duties of non-intervention should be modified to include a broad definition of "coercion."*

Although they overlap in many respects, the principal of non-intervention is somewhat easier to apply to cyber-attacks than the principles of sovereignty. On its face, non-intervention is a better fit for cyber-attacks because it lacks the physical territory element that breach of sovereignty requires. However, a few changes to non-intervention could still make it apply more cleanly.

The first requirement – an act bearing on matters that each state is free to decide – seems relatively easy to meet for most types of cyber-attacks.[150] Scholars have extended this category to generally include state organization as something that a state may freely decide.[151] Thus, a state's electoral, political, and economic systems, for example, are each something that it freely chooses.[152] Since electoral and economic systems are large pieces of a state's freely chosen organization, a cyber-attack on a state's elections or economy would likely meet the first requirement.[153] However, the second requirement – coercion – poses several issues. For one, the precise scope of "coercion," as used by the ICJ

150. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).

151. *See* Nicar. v. U.S., 1986 I.C.J. ¶ 205; *see* TALLINN MANUAL 2.0, *supra* note 79, at 315.

152. Nicar. v. U.S., 1986 I.C.J. ¶ 205; *see* TALLINN MANUAL 2.0, *supra* note 79, at 315.

153. *See* G.A. Res. 36/103, annex (Dec. 9, 1981) (stating that non-intervention includes (1) "the right of States and peoples to . . . use their information media in order to promote their political, social, economic and cultural interests and aspirations," (2) "the duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States," and (3) "[t]he right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news which can be interpreted as interference in the internal affairs of other states or as being harmful to the promotion of peace, co-operation and friendly relations among states and nations.").

here, is disputed.[154] Most states have defined this element as physically forcing a state to do something.[155] Some, however, have urged that coercion actually is meant to be read as also including political or economic "influence" on the state's behavior.[156] While the strict "force" definition can be applied to cyber-tampering in the sense that one state is forcing the other to turn over data by simply stealing it, the broader "influence" definition would be the most viable avenue for the law to apply to cyber-influencing. This is because there are a variety of motivations that states may have for interfering in elections or economies, and each would fall under this broader umbrella of seeking to "influence" another state's political or economic affairs.[157] Thus, "coercion" would need to be defined in the Articles on State Responsibility as including the "force" definition as the general definition, as well as a broader "influence" definition that specifically applies to cyber-influencing. However, this definition needs to be narrowly tailored to interferences in a state's elections or economy, because otherwise it risks looking like the SCO's definition of cyber-attack and putting citizens at risk.

iii. *The duty of due diligence is likely unworkable because it may be difficult to locate the source of a cyber-attack and the consequences can be hard to measure.*

---

154. TALLINN MANUAL 2.0, *supra* note 79, at 317 (stating that international law does not have a strict definition of coercion).

155. Sander, *supra* note 78, at 24 (discussing the difficulties of concluding cyber influence on elections as a prohibited form of intervention because traditionally, international law results from examples of physical actions).

156. *See, e.g.*, Bowett, *supra* note 81, at 248–49 (explaining that coercive actions are broad in that they usually entail economic influence or impact and that the line between economic and political motives is unclear, so if political influence is allowed through coercion, then regulation of economic coercion is unlikely).

157. *See* TALLINN MANUAL 1.0, *supra* note 49, at 45, 47 (defining prohibited forms of intervention as including "the manipulation by cyber means of elections or of public opinion on the eve of elections, as when online news services are altered in favour of a particular party, false news is spread, or the online services of one party are shut off"); *see also* Buchan, *supra* note 148, at 78, 80 (stating that "conduct which compromises or undermines the authority of the state should be regarded as coercive," including when State data is simply "accessed and appropriated" by a cyber-attacker).

As written, the due diligence duty is also not cleanly applicable to cyber-attacks.[158] The principle of due diligence is the weakest of the three state responsibility principles and would require the most modification. The first element – knowledge – requires actual knowledge and seems to depend on the scenario.[159] If a state is responsible for an attack, it will necessarily have knowledge of the cyber operation. If a state is not responsible for an attack, it likely will not have knowledge of the operation and domestic cyber-crime laws may be more applicable in the first place. Alternatively, a state may be knowingly harboring a cyber-attacker in order to scramble responsibility. In this case, the knowledge element clearly matters. But even if a state knows a cyber-attacker is commencing attacks within its borders, it is still often unclear who is behind it.[160] As discussed above with attribution issues under the U.N. Charter, cyber-attackers often work remotely or disguise their identities and locations.[161] In this sense, this duty may needlessly impose multiple layers of liability upon states.[162] If a cyber-attack is threaded through servers or other technology located in multiple countries, multiple parties could be accused of failing to take reasonable measures to end an attack. But as noted, this may simply be an unavoidable consequence of the nature of cyber operations.

---

158. *See* TALLINN MANUAL 1.0, *supra* note 49, at 206 (noting that, like sovereignty, the duty of due diligence is also contested among international communities as to whether it is an international legal obligation in the cyber-attack context).

159. *See id.* (clarifying that there is no consensus on whether this standard applies with only constructive knowledge).

160. Chircop, *supra* note 141, at 666–67 (stating that the uncertainty and anonymity of the cyber-sphere hinders the emergency of a clear State practice regarding the application of due diligence to cyber-attacks).

161. *See* Waxman, *supra* note 30, at 447 (discussing how cyber-conflict is likely to exacerbate the already-existing challenges posed by proxy wars because actors can more easily "mask or anonymize their identity and because the 'movements' and 'terrain' of cyber-warfare can be dispersed across global information networks and will often be carried out on private infrastructure").

162. *See id.* at 448 ("[C]yber-warfare may lack clearly discernible starting points and readily observable or provable actions and counter-actions."); Chircop, *supra* note 141, at 650 ("[A] natural concern with accepting a due diligence standard of attribution is that it would lead to indeterminate liability for states.").

The second element – failure to take reasonably feasible measures to end the attack[163] – can pose issues in the cyber-attack context because, in the case of a complex and well-executed cyber-attack, it can be unclear what "reasonably feasible measures to end the attack" means. As a result, if due diligence were to be applied, a state may be held responsible for a cyber-attack when it can be traced to its territory, but it may not have the means or even know how or where to stop the attack.[164] This too can needlessly impose liability on a victim state, when the real target is the person executing the cyber-attack.

The third obstacle is the principle's requirement that the act be contrary to the state's rights.[165] Similar to the attribution obstacle, this requirement is easier to meet in the cyber-tampering context. It's much easier to show that a data breach is a violation of a state's national secrets and more on par with espionage. With cyber-influencing, however, the line is much less clear. The best argument is that a state's political and economic sovereignty is a state right and that any degree of interference with either of these amounts to an act contrary to the state's rights. But, recall that this would be entirely dependent upon whether or not sovereignty is redefined to broadly include digital territory and damage to political and economic integrity.

The next element – "serious adverse consequences"[166] – is also not particularly helpful when dealing with cyber-attacks. This is because the seriousness of cyber-influencing can be extremely hard to measure without some sort of tangible injury.[167] As stated, physical injury is not likely if the attacker is only utilizing cyber-influencing operations. Thus, as above, cyber-tampering is much easier to reconcile with this definition because, for example, it can result in national security threats if military data is breached (think, as an extreme example, if nuclear access codes are hacked or if power grids are shut down nationwide), and it can result in massive privacy breaches, both in terms of individual citizens and

163. Sander, *supra* note 78, at 25.

164. Nicholas Tsagourias, *Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts*, 21 J. OF CONFLICT & SEC. L. 455, 466 (2016).

165. Sander, *supra* note 78, at 25–26.

166. *Id.* at 26.

167. *Id.*

large corporations that all possess rights to certain private information.[168] The consequences of cyber-influencing on the other hand are much more difficult to quantify. One argument is that which was applied to sovereignty: measure the damage through audience reach. However, while this provides a way to quantify a consequence, it provides no clarity for whether that consequence was "serious" or "adverse." Who is to say that the cyber-influencing negatively impacted American minds? Who is to say that it made a noticeable difference at all? Even if millions of people were exposed to the attack, that is not dispositive of whether or not it impacted them or ultimately influenced the election or economy. Thus, as a result of these largely unquantifiable attributes, the duty of due diligence, even with modifications, like would still be inapplicable to cyber-attacks.

Overall, neither the pre-existing U.N. framework nor the duties under the customary international law principle of state responsibility are well suited as written for all cyber-attacks. Both would need to be tailored in at least a few areas in order to be workable, and even then, the duty of due diligence would likely be incompatible with cyber-attacks.

III. CONCLUSION

The current state of international law is insufficient to address cyber-attacks, leaving countries vulnerable to cyber-attacks without recourse, and leaving countries with powerful cyber-capabilities free to attack with essentially no direct threat of international legal punishment. The seemingly never-ending counterattacks that countries like the U.S., China, and Russia have been carrying out against each other over the past few years demonstrate the result of a missing applicable legal framework. As the law currently stands, there are several gaps that must be filled in order for it to be applicable to cyber-attacks, and

168. *See* Sander, *supra* note 78, at 38 (mentioning breaches of privacy as a potential result of cyber doxing operations). As a side note, interference with power grids is not as unlikely as it may sound. In December 2012, two U.S. power plants were compromised through something as simple as unprotected and infected USB drives, and in May 2013, the Department of Homeland Security reported that U.S. electrical grids were being constantly probed by multiple state actors, including Iran. *Significant Cyber Incidents*, *supra* note 3.

essentially all U.N. member states recognize this. How exactly to fill those gaps though, is greatly contested. The U.S. must directly compete with SCO-member countries like China and Russia to have its definitions and interpretations of the U.N. Charter and international principles of state responsibility put into effect. The U.S. pushing for definitions and interpretations that both maintain the statute of the current international laws, but do not degrade human rights, is imperative not only for its own domestic interests, but also to ensure that rights to free expression and association are protected around the world.

This paper has suggested several modifications. First, an additional cyber-specific definition of "armed attack" based on the U.S. definition of cyber-attack is needed to make the U.N. Charter workable. Second, codifying the inclusion of cyber-space in the definition of "territory" is necessary to make the principle of sovereignty applicable. Third, broadening the term "coercion" to include political and economic coercion conducted by through cyber means, again based on the U.S. definition, is necessary to make non-intervention workable. If the U.S. is unable to cultivate agreement among other U.N. member states on these or similar changes, electoral interference in future elections will be entirely undeterrable and unpunishable under international law, and the United States' only option will be to counteract cyber-attacks with its own cyber-attacks. This, however, would do nothing to limit the effects that cyber-insecurity during another U.S. election would have on the American electoral system, and the trust that American citizens hold in the validity of the electoral results. Thus, because cyber-warfare has seemingly outpaced international law, it is time for the law to catch up.