PROLIFERATION OF CYBERWARFARE UNDER INTERNATIONAL LAW: VIRTUAL ATTACKS WITH CONCRETE CONSEQUENCES

MAXWELL MONTGOMERY✠

I. INTRODUCTION

Looking back on nearly every technological advancement of our society, such groundbreaking technologies are typically accompanied by a myriad of benefits that make life easier, but seldom are the consequences of these breakthroughs anticipated or considered. Often times, these innovations are developed and intended for productivity and advancement, and yet they open the door for potential harm by those who want to use the technology for power or violence. With the rise of computers and the Internet, technology has created a unique network of interconnectedness that could not have been imagined even just a few decades ago. Problems arise, however, when this technology creates opportunities for acts of aggression or malevolence that are both incredibly hard to isolate and also fall outside the status quo of military and state engagement in traditional warfare.

Cyberwarfare is not easily defined and part of this difficulty resides in the fact that unlike conventional warfare, cyberwarfare takes place beyond our tangible borders and is not always easily attributable to specific state actors. While it may be easy to classify an act of war when a country is invaded or attacked by enemy troops, this question becomes more complicated and convoluted when there are no bullets or bombs, or an identifiable state sponsor of such malicious activity. To complicate this matter further, there is still no international consensus concerning how to address this growing issue. The traditional rules for engagement and defense under international law neither acknowledge the unique nature of cyberwarfare nor yield direct answers for how a nation may be justified in retaliating if it is attacked.[1] This paper seeks to highlight the complicated nature of cyberwarfare in today's geopolitical climate as it might be analyzed under current international law, and considers what changes could be made to address this new and growing platform for international aggression and defense.

This paper will begin with a general overview of cyberwarfare today and will highlight various methods of cyberattacks that nations and individuals have used in recent history. These different categories will be paired with

✠. Class of 2019, University of Southern California Gould School of Law; B.A. English Writing, Loyola Marymount University; Staff, *Southern California Interdisciplinary Law Journal*. The author would like to thank the staff and editorial board of the Southern California Interdisciplinary Law Journal for their hard work assisting with this note, and Professor Josh Lockman for his guidance.

1. *See* NILS MELZER, CYBERWARFARE AND INTERNATIONAL LAW 4 (2011).

recent examples of each method that have been employed internationally. After discussing the differences between these different types of cyber-activities, the analysis will then shift to focus on the difficulties in determining a universal definition of cyberwarfare, and the legal ramifications that come with this problem.

In the next section, the discussion will begin to focus in on the legal framework involving a nation's legally justified options when faced with a severe cyberattack. At present, there is no clear doctrine or contingency plan in place, as there has yet to be a sufficiently catastrophic cyberattack to warrant a military response. This paper will adopt the charter of the United Nations as a framework to analyze this issue from a legal perspective. This analysis will begin with the general prohibition on a nation's use of force against another, and explain the circumstances when a state may create an exception to this prohibition. Specifically, this paper will analyze when a nation might justifiably retaliate against another nation or individual through military action or a counter-cyberattack. The analysis will focus on the difficulties in using this doctrine as applied to cyberattacks, since cyberwarfare was not a consideration when the charter was drafted decades ago. Multiple issues make this analysis complicated and imperfect, and this paper will suggest the best method to use when analyzing these attacks under the international legal doctrine.

Ultimately, this paper will conclude that the current framework must be adapted to include cyberattacks and a clear methodology for analyzing this new form of technological warfare. Unless a clear doctrine is outlined by the international community to address instances when a nation would be legally justified in responding with military action, it is likely that this ambiguity in the law will result in either increased escalation and proliferation of cyberattack activities, or an unprecedented military response to such activities with severe consequences.

II. DEFINING AND DISTINGUISHING CYBERATTACKS

Before analyzing how cyberwarfare may be addressed under international law, one must consider the wide scope of activities that could be encompassed by this label, and how these actions might be interpreted by a nation on the receiving end of such an attack. In a broad sense, a cyberattack may be defined as "the use of deliberate actions—perhaps over an extended period of time—to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[2] These attacks are difficult to classify and analogize with traditional methods of warfare because of the various methods and differing degrees of severity.

The U.S. Department of Defense has classified cyberwarfare activities as computer network operations (CNO) and has broken these down into three general categories: computer network attacks (CNA), computer network

2. KENNETH W. DAM ET AL., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 80 (William A. Owens ed., 2009).

exploitation (CNE), and computer network defense (CND).[3] While these classifications may be helpful in separating various types of cyber activities, there is no international consensus delineating how the varied nature of these cyber activities fits within the law. Thus, it remains unclear where to draw the line between activities that may be classified as espionage or defensive tactics, and actions that might be considered acts of aggression or even acts of war. This line between defensive and offensive conduct is much more recognizable in traditional combat than it is in cyberwarfare, and this presents many issues. One reason for this blurry distinction is the fact that in most instances, when a nation realizes that its network has been breached or manipulated, it is unclear whether this breach was done merely out of defensive or deterrent action, or in preparation for further acts ultimately leading to real warfare.[4] With this blurred distinction comes the more significant ambiguity regarding whether or not a nation may respond militarily if their network is breached and attacked.

Various recent examples of cyberattacks illustrate the difficulty in classifying these operations as either acts of war or exercises of deterrence and defense. Nations routinely engage in cyber-activities and espionage, and these actions vary in degrees of seriousness and potential for backlash.[5] Some common examples of cyberattacks include: infrastructure sabotage, denial of service, sleeper malware,[6] phishing,[7] and implanting false information.

A. INFRASTRUCTURE SABOTAGE

One of the most prominent examples of cyberattacks involving infrastructure sabotage was the Stuxnet program—an invasive network "worm" that the United States and Israel allegedly used to target Iran's nuclear facilities.[8] After infiltration, and once it infected the computer network, Stuxnet caused the nuclear centrifuges to malfunction and fail.[9] While the U.S. and Israel have not officially claimed responsibility, the complexity of the program was so advanced that it is unlikely to have been

3. *See* MELZER, *supra* note 1, at 5 ("While computer network attacks (CNA) comprise all cyber operations aiming 'to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves', computer network exploitation (CNE) refers to '[e]nabling operations and intelligence collection to gather data from target or adversary automated information systems or networks'. Computer network defence (CND), in turn, refers to '[a]ctions taken to protect, monitor, analyse, detect, and respond to unauthorized activity within . . . information systems and computer networks' or, in short, the prevention of CNA and CNE through intelligence, counterintelligence, law enforcement and military capabilities.").

4. *See* Alyza Sebenius, *Writing the Rules of Cyberwarfare*, ATLANTIC (Jun. 28, 2017), https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/.

5. *See* Damian Paletta et al., *Cyberwar Ignites a New Arms Race*, WALL ST. J. (Oct. 11, 2015, 8:52 PM), https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128.

6. *Id.* ("Edward Snowden leaked documents that showed that the NSA had implanted malware on tens of thousands of foreign computers. That allowed the U.S. government secret access to data and, potentially, the industrial control systems behind power plants and pipelines.").

7. *Id.* ("'[P]hishing' [is] sending a flood of disguised emails to trick corporate employees and government bureaucrats [in]to letting them into their networks.").

8. *See* Sebenius, *supra* note 4.

9. *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

directed by any other nation with as strong of an interest in deterring Iran's nuclear capability.[10] Analysts who have tried deconstructing the Stuxnet virus have concluded that it is most likely the product of a very sophisticated effort to target these Iranian networks, as the worm actually spread to thousands of other computers worldwide, but only caused damage to the networks in Iran.[11] The "worm" was purportedly delivered directly into the secured network by means of a thumb drive, and once it infected one computer, it spread within the network and caused significant damage to Iran's nuclear networks.[12] While this was an incredibly effective method of deterrence against Iran's nuclear capabilities and could be classified as a defensive measure by the United States and Israel, it is easy to see how Iran might consider this an overt act of aggression and hostility with justification for retaliation. By way of further exaggerating what could have happened, if a nuclear reactor would have melted down and caused significant civilian harm, this cyberattack would have been on par with a traditional nuclear strike, with the U.S. as the aggressor. Unlike many other types of cyberattacks, this operation illustrated that malware on a computer can cause drastic physical damage to enemy infrastructure, and potentially even to an extent equivalent to a traditional military strike.

B. DISTRIBUTED DENIAL OF SERVICE (DDOS)

A distributed denial of service (DDOS) is another commonly known type of cyberattack that could cripple a nation's ability to communicate or access information for extended periods of time.[13] This is exactly what happened in 2007, when Russian hackers were allegedly involved in a distributed denial of service hack, which shut down portions of the Internet in Estonia, and limited communication channels in the country.[14] This attack was prompted

10. Paletta, *supra* note 5 ("[T]he Stuxnet computer worm . . . [is] considered to be the most successful and advanced cyberattack ever. The U.S. and Israel haven't confirmed or denied involvement with Stuxnet.").

11. John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. MARSHALL J. COMPUTER & INFO. L. 1, 6 (2011) ("Individuals who have spent significant time trying to understand the Stuxnet code via reverse-engineering report that 'its level of sophistication suggests that a well-resourced nation-state is behind the attack. . . . On top of that, 'the worm's pinpoint targeting indicates the malware writers had a specific facility or facilities in mind for their attack, and have extensive knowledge of the system they were targeting.'").

12. *Id.* at 5 ("[T]he malware was initially distributed 'via an infected USB thumb drive memory device' or devices, 'exploiting a vulnerability' in the Microsoft Windows operating system. Indeed, 'such systems are used to monitor automated plants—from food and chemical facilities to power generators. Analysts said attackers may have chosen to spread the malicious software via a thumb drive because many [Supervisory Control and Data Acquisition ("SCADA")] systems are not connected to the Internet, but do have USB ports.' Further, once the system is infected, the worm 'quickly sets up communications with a remote server computer that can be used to steal proprietary corporate data or take control of the SCADA system . . . .'").

13. *See* Emily Tamkin, *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* (Apr. 27, 2017, 8:30 AM), http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/ ("[A] Distributed Denial of Service Attack [is] an orchestrated swarm of internet traffic that literally swamps servers and shuts down websites for hours or days.").

14. *Id.* This attack was in response to Estonia's decision to remove a Soviet WWII statue from its capital. ("The Russian government had warned that removing the statue would be 'disastrous for Estonians,' but since Moscow no longer called the shots in the Baltic state, the statue was duly shipped off to a suburban military cemetery. Soon after, Estonians found that they couldn't use much of the

by the removal of a Soviet statue from the capital of Estonia, which resulted in riots and even an attack against the Estonian embassy in Russia.[15]

The cyberattack against Estonia lasted weeks and involved many different elements. The attack involved manipulation of Estonian websites by removing content and replacing it with Russian propaganda, completely shutting down popular sites (including government sites), shutting down the country's top news outlet, and overwhelming critical networks used for cellular networks.[16] This attack left Estonians completely cut off from the outside world, and illustrated how a society can be thrust into chaos when its reliance on computer networks is exploited by an outside agent with nefarious intentions.[17] Just one year later, Russia executed another cyberattack against Georgia using the same method of distributed denial of service, this time isolating the country's communication abilities in conjunction with sending Russian military forces to invade the country.[18] In this attack, Russia demonstrated how effective this type of cyberattack can be when executed along with traditional armed forces, leaving the victim's government confused and crippled as it is being invaded.[19] While typically these kinds of attacks are mainly an inconvenience to the victims like the example involving Estonia[20], this kind of service disruption can lead to significant hardship and civil chaos if the service denial persists for a long period of time, or if enough critical services are hampered by the cyberattack.

C. IMPLANTING FALSE INFORMATION

One final example of a prominent cyberattack method is planting false information. This can occur in different ways, but commonly these attacks will either suppress information that is true, or project information that is false. Typically this is done with radar manipulation, which can cause an enemy system to hide approaching forces or to falsely show incoming enemy forces when there are none.[21] These attacks are so effective because the attacked computer system appears to be operating correctly, when in fact it has been drastically compromised, and by the time the victim recognizes

internet. They couldn't access newspapers online, or government websites. Bank accounts were suddenly inaccessible."). *Id.*

15. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 205 (2009).

16. *Id.* at 206.

17. *See* Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare,* 106 MICH. L. REV. 1427, 1429 (2008) ("Hitting the websites of banks, ministries, newspapers, and broadcasters, the assault left Estonia without the means to tell the world it was under attack. The strike was both indiscriminate and surprisingly focused: 'Particular "ports" of particular mission-critical computers in, for example, the telephone exchanges were targeted. . . .' This attack was more than just an inconvenience to the Estonian population: the emergency number, used to call for ambulances and the fire service, was unavailable for more than an hour.").

18. Tamkin, *supra* note 13, at 2.

19. Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B. C. INT'L & COMP. L. REV. 439, 443 (2009).

20. Richardson, *supra* note 11, at 14 ("However, in the case of the Estonia attack, there were nine deaths directly attributed to the cyber intrusion. This was not because of some external pressure, a blockade, or sanctions, but a disruption that occurred from actions within the borders of these two states.").

21. *See* Paletta, *supra* note 5, at 8.

what is happening, it is likely too late.[22] A recent example of this type of attack was executed by Israel in a strike against a suspected nuclear material facility in Syria.[23] In this attack, Israel was able to isolate Syrian air defense systems and feed false information into the radar system to show that there were no approaching planes, allowing the Israeli Air Force to attack the target undetected.[24] Unlike most other cyberattacks, these methods are typically more easily attributable because the cyberattack is usually executed in conjunction with a tangible military force behind it.[25]

The range of cyberattacks is not limited to these few common methods, but it is apparent that there are blurred lines distinguishing how these acts might be interpreted. Currently, the international community has not reconciled an objective standard to weigh these types of attacks in determining whether or not a country would be justified in responding militarily. While it might be difficult to create a bright line objective distinction, a dialogue must begin regarding this issue so nations are better equipped to respond to actions that may cross the line into an act of war. Without a clearer picture of how states are permitted to respond to these attacks, this environment is ripe for escalation and increasingly invasive and destructive tactics being developed by countries around the world.

III. CYBERWARFARE AND INTERNATIONAL LAW

While the U.N. Charter created a framework for the law of war, or *jus ad bellum*, it lacks a clear doctrine for how a nation should proceed after a substantial cyberattack from another state's aggression.[26] The lack of a legal doctrine defining cyberwarfare may open the door for serious disputes concerning states' right to respond to attacks with military action. Still, any legal analysis of cyberwarfare is perhaps best addressed through the U.N. Charter. Under Article 2(4) of the Charter, "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[27] While the scope of this article can be interpreted in varying degrees of specificity, generally this prohibition has not been applied to uses of force that fall outside of conventional military attacks, like enacting sanctions with the purpose of

22. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 839 (2012); *see also* Paletta, *supra* note 5 ("Air Force Chief of Staff Gen. Mark A. Welsh III told a group of reporters in April that he wanted to see the military develop 'blunt force trauma' powers with their cyberweapons. He gave examples of computer codes that could 'make an enemy air defense system go completely blank' or have an enemy's 'radar show a thousand false targets that all look real.'").

23. *See* Sharon Weinberger, *How Israel Spoofed Syria's Air Defense System*, WIRED (Oct. 4, 2007, 3:14 PM), https://www.wired.com/2007/10/how-israel-spoo/.

24. Hathaway et al., *supra* note 22, at 838; *see* Weinberger, *supra* note 23 ("The process involves locating enemy emitters with great precision and then directing data streams into them that can include false targets and misleading messages algorithms that allow a number of activities including control.").

25. Hathaway, *supra* note 22, at 838.

26. Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1040, 1042 (2007) ("Nevertheless, the gap between physical weaponry (whether kinetic, biological, or chemical) and [cyberwarfare's] virtual methods can be substantial, creating acute translation problems. Attempts to apply existing principles to [cyberwarfare] result either in no clear rules emerging or a rule that contravenes other principles fundamental to the law of war.").

27. U.N. Charter art. 2, ¶ 4.

causing severe economic distress or hacking into foreign networks to cause damage or gather reconnaissance.[28] Because it has not yet been directly addressed, before determining what actions a state might take in response to a cyberattack, we must first determine whether a cyberattack could ever reach the threshold under the U.N. Charter constituting a "use of force." While simplistic in the idea it expresses, Article 2(4) is ambiguous and can be interpreted in many different ways when considering what exactly might constitute a prohibited "use of force."[29]

Historically, Article 2(4) has been interpreted to be a prohibition on military force and armed violence, rather than other uses of force such as economic and political pressures exerted on another nation. This interpretation does have some historical contextual support, as the Charter was ratified after World War II, and set out to limit a nation's ability to start a legally justified war under international law.[30] There is some hesitation among scholars in expanding the interpretation of "use of force" to actions that fall outside the traditional measure of armed force.[31] The most common view, and that taken by the United States, is that Article 2(4) only refers to traditional military attacks and armed violence against another nation.[32]

Some scholars have considered an expanded definition of improper force, focusing on the impact of the state's action, particularly coercion, rather than relying on the instrument or methodology for exerting force.[33] For years, less influential countries have argued to expand this definition to include economic and political coercion, sanctions, and funding of militant groups, but thus far the U.N. has rejected such an interpretation, instead relying on the traditional understanding of armed force.[34] Similar to the

28. *See* Hathaway, *supra* note 22, at 842 ("The precise scope of the international prohibition on the threat or use of force has been the subject of intense international and scholarly debate. . . . Nonetheless, the general consensus is that Article 2(4) prohibits only armed force.").

29. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 427 (2011) ("Article 2(4)'s express prohibition is both straightforward and ambiguous. It is direct and absolute on its face, yet, . . . 'the paragraph is complex in its structure[,] and nearly all of its key terms raise questions of interpretation. . . .' [N]ew technologies raise interpretive puzzles with echoes of previous eras.").

30. Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207, 215–16 (2002) ("After World War II, the leaders of the dominant world states attempted to create an international system that would promote a lasting peace. The result was the United Nations and its founding document, the U.N. Charter. Like the League of Nations that preceded it, the United Nations limited the legality of a nation's ability to resort to war. The first purpose of the United Nations, according to Article 1 of the U.N. Charter, is to maintain international peace and security through collective measures and to block acts of aggression or breaches of the peace.").

31. *See* Hoisington, *supra* note 19, at 447.

32. Hathaway, *supra* note 22, at 838; Waxman, *supra* note 29, at 427 n.25 ("Traditional [law of armed conflict] emphasizes death or physical injury to people and destruction of physical property as criteria for the definitions of 'use of force' and 'armed attack.'").

33. Waxman, *supra* note 29, at 428.

34. *Id.* at 428–29 ("This interpretation of Article 2(4) stresses its purpose over its text. At various times, some states—usually those of the developing world, and, during the Cold War, often with Soviet bloc support—pushed the notion that 'force' includes other forms of pressure, including political and economic coercion threatening to state autonomy."); Hoisington, *supra* note 19, at 447 ("[D]espite attempts by developing states to include economic coercion within article 2(4) during the drafting of the Charter, such practices have been expressly excluded. Thus, analysis based on either the text of article

coercion interpretation, some have considered interfering with another nation's sovereignty or intervening in its political system to meet the requisite measure of "force" within Article 2(4).[35] An example of such an act would be supplying funding or weapons to a nation's rebels during a coup, or dropping information or propaganda into a closed nation like North Korea.[36]

However, there has been some pushback to expanding the interpretation of "force" under the Charter. Opening the door for a broader definition of force, including non-kinetic uses, could cause problems with this framework and allow countries to be legally justified in starting a war without actually being "attacked."[37] Often times, political and economic coercion is used as an alternative to traditional conflict and military engagement, so there is some speculation that lowering the standard could actually increase instances of armed conflicts.[38]

Among theses various approaches, the historical context seems most reasonable overall, but relying solely on historical context is not entirely adequate in the realm of cyberwarfare. The drafters could not have imagined anything similar to the Internet or cyberwarfare at the time the Charter was written. While it would be too inclusive to expand the "force" definition to include all instances of cyberwarfare, one can imagine a situation where a network attack could cause significant damage, similar to a traditional military attack. This issue will be discussed further in this paper but does not have a clear-cut solution or a consensus among scholars.

Putting aside the ambiguity of what constitutes "force," the Charter's prohibition on uses of force in Article 2(4) is limited by two very important exceptions. The first falls under Article 39, which allows the U.N. Security Council to authorize military action in response to a state's improper use of force.[39] The second exception guarantees a sovereign state's irrevocable

---

2(4) or the history underlying its adoption requires an interpretation excluding economic, and for that matter political, coercion from the article's prescriptive sphere.").

35. Waxman, *supra* note 29, at 430 ("States advocating expansive interpretations of prohibited force that would include subversion sought to hermetically seal their domestic system from outside interference while still participating in the broader international political community. In a similar way, some states today want the benefits of international informational connectivity while insulating their computer and communication networks from outside influences or intrusions deemed hostile or undermining.").

36. *See id.* ("Like past efforts to define Article 2(4) 'force' as coercion, efforts to expand its coverage beyond armed force so as to include violations of sovereign domain such as propaganda or political subversion never gained significant traction. Pragmatic considerations precluded the much broader interpretation, though this alternative approach raises the question of whether cyber-attacks might be analogized to other covert efforts, like propaganda campaigns, to undermine political or economic systems.").

37. Hoisington, *supra* note 19, at 447 ("Such an expanded definition of the use of force would make it very difficult to continue to exclude acts of coercion from article 2(4) because international law would have to distinguish cyberattacks that do not cause physical damage, such as electronic incursions and blockades, from acts of economic and political coercion, such as economic sanctions, which traditionally and specifically have been excluded from article 2(4), but which may often have the same effect.").

38. *See* Waxman *supra* note 29, at 429 ("One problem with this approach has always been the difficulty of distinguishing unlawful coercion from lawful pressure. After all, coercion in a general sense is ever-present in international affairs and a part of everyday diplomacy and statecraft.").

39. U.N. Charter art. 39.

right to defend itself after being attacked.[40] These provisions of the U.N. Charter have been used throughout history to justify military action, but have thus far never been called upon in response to a cyberattack. With the evolving landscape of conflict and the growing occurrences of cyberattacks, this gap in application will need to be addressed. Otherwise, nations with malicious intentions will be able to relentlessly attack computer networks, while remaining protected by the ambiguity in international law regarding cyberattacks as uses of force under this doctrine.[41]

A. U.N. CHARTER ARTICLE 39 – SECURITY COUNCIL INTERVENTION

While nations are generally prohibited from using or threatening to use force against other member nations, Article 39 creates an important exception in which the use of force will be legally justified under the U.N. Charter. Article 39 of the Charter states that "[t]he Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."[42] Article 39 effectively operates as a check against nations unilaterally intervening and starting conflicts, instead creating an administrative body responsible for determining when a breach of the peace or an act of aggression has occurred.[43] The U.N. Security Council is made up of fifteen members, including five permanent members and ten non-permanent members who are voted in by the General Assembly and serve two-year terms.[44]

Article 39 provides that the Security Council may determine in its discretion whether or not a state's action has created a breach of the peace or an act of aggression. However, much like the ambiguity addressed earlier in Article 2(4), there lacks a clear consensus of what kind of state action would meet this threshold to warrant joint action by the Security Council.[45] This process is often perfectly adequate for acts consistent with conventional kinetic warfare, as the Security Council can easily identify if a country is under attack by an aggressor nation. There would be little speculation about whether or not an armed invasion would constitute a breach of peace under

40. *Id.* at art. 51.

41. *See* MELZER, *supra* note 1, at 8 ("As a matter of logic, the Charter cannot allow that the prohibition of interstate force be circumvented by the application of non-violent means and methods which, for all intents and purposes, are equivalent to a breach of the peace between the involved states.").

42. U.N. Charter art. 39.

43. *See* Jensen, *supra* note 30, at 217 ("In other words, the U.N. Charter authorizes the Security Council to determine the nature of a nation's actions and to decide what preventive or remedial actions are appropriate. . . . By delegating this determinative power, the U.N. Charter has removed it from each individual nation except to the extent provided in Article 51 for self-defense.").

44. *Current Members*, U.N. SEC. COUNCIL, http://www.un.org/en/sc/members/. The five permanent members are China, France, Russian Federation, United Kingdom, and the United States.

45. John Dever & James Dever, *Cyberwarfare: Attribution, Preemption, and National Self Defense*, 2 J.L. & CYBER WARFARE 25, 33 (2013) ("While the U.N. Charter allows for the U.N. Security Council to declare whether a specific act constitutes a threat to the peace, breach of the peace, or an act of aggression, there are no definitions of these specific terms in the Charter itself, and it is left up to the U.N. Security Council to determine both what these terms mean, and whether a particular action fits into one of these categories.").

the Charter to warrant joint action against the aggressor. An example of Security Council intervention occurred in 1990, when Iraqi forces breached the peace and invaded Kuwait.[46] After Iraq invaded Kuwait, the Security Council denounced the action and voted nearly unanimously to condemn the act of aggression, threatening to enact severe sanctions against the nation unless it immediately removed all troops from the region.[47] In this case the Security Council was able to promptly hold a vote, and effectively counter Iraq's aggression in a diplomatic way.[48] Throughout the Charter's history, Article 39 has only been exercised a few times, but in cases of traditional military aggression, it has been effective both as a deterrent and as a response.[49]

Like many other issues mentioned thus far, the line defining what amounts to force or aggression is blurry with cyberwarfare. In a prospective cyberattack, it would be incredibly difficult, if not impossible, to pinpoint the actor responsible, diagnose the extent of the damage, and vote whether or not the intrusion or attack crossed the threshold to be considered a breach of the peace and require the Security Council's intervention. Essentially, this forces the Security Council to diagnose the severity of a cyberattack, make a judgment call on an appropriate response, and then authorize such a response, all while the victim nation's infrastructure and computer networks may be completely destroyed or compromised.[50] Ignoring the inherent difficulty in tracking the source of a cyberattack, it is likely that many nations would be uncomfortable and unwilling to turn over evidence of the attack. Such a disclosure to the Security Council might result in leaking of confidential information or source code that could potentially be used against that nation in the future. Because of this, a nation is probably less likely to seek Security Council assistance in the wake of a serious cyberattack, and might instead choose to retaliate unilaterally. Without an international consensus about what kind of action should trigger Article 39 in the world of cyberattacks, nations will likely decide to respond to such attacks without regard to whether the response is appropriate under Article 39 and before the Security Council can process what actions to take.[51]

For many of the reasons outlined above, Article 39 realistically has limited applicability in the cyberwarfare context, as it would require administrative hurdles, involving garnering support from the Security Council, and securing requisite votes to determine if a cyberattack has

46. Jensen, *supra* note 30, at 217.

47. Paul Lewis, *The Iraqi Invasion; U.N. Condemns the Invasion with Threat to Punish Iraq*, N.Y. TIMES (Aug. 3, 1990), http://www.nytimes.com/1990/08/03/world/the-iraqi-invasion-un-condemns-the-invasion-with-threat-to-punish-iraq.html.

48. *See id.*

49. *See id.* ("[P]revious occasions were the imposition of arms embargos against South Africa and Rhodesia, the threat of sanctions to obtain a cease fire ending the first Israeli-Arab war in 1948, and and [sic] the council's action ordering a cease-fire in the Iran-Iraq war in 1987.").

50. Dever & Dever, *supra* note 45, at 34 ("Although the determination about whether a cyberattack constitutes an act of aggression under Article 39 is a policy decision by the Security Council it would provide greater clarity in the international context if there were a more clearly defined standard, which separates in a distinct manner armed attack, aggression, and use of force.").

51. *Id.* at 33 ("The failure to have clear definitions makes it difficult for states to determine whether their actions are allowed by the Security Council prior to actually committing the actions. This is particularly true in the context of an emerging field, such as cyberspace.").

reached a level of severity sufficient to cause a breach of peace within the United Nations. Due to the urgent nature of cyberattacks and the immediate consequences that can quickly escalate, exercising this right under Article 39 offers limited assistance or guidance to a nation suffering a crippling cyberattack.

B. U.N. CHARTER ARTICLE 51 – RIGHT TO SELF-DEFENSE AFTER AN "ARMED ATTACK"

The more practical legal analysis for cyberwarfare under the U.N. Charter would be derived from Article 51, which ensures that "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 the measures necessary to maintain international peace and security."[52] This Article in the Charter explicitly promotes the inherent right of a nation to defend itself if it has been attacked by an aggressor.[53] Under this doctrine, the main issue that must be considered is whether a cyberattack could ever reach a level of severity where it could be considered an "armed attack" under the meaning of Article 51. While this question of force was considered generally in regards to Article 2(4) and Article 39, in the instance of Article 51, the standard is likely a higher burden than the "use of force" or "breach of peace" considered previously. If you asked a textualist whether or not a cyberattack would meet this threshold of an "armed attack", that answer would appear to be a simple "no," and it may be difficult to argue that "armed attacks" could extend to cyberattacks conducted over computer networks with no weapons involved. However, a textual interpretation is inadequate here, as it has become evident that while executed over servers and networks, certain cyberattacks have the capacity to cause devastating damage and significant loss of life if the right systems are targeted. It is not likely that the U.S. would be restrained by this language in defending itself if, for example, a cyberattack caused one of our nuclear reactors to meltdown and harm civilians. At present, there lacks international consensus and legal precedent regarding how to address instances of cyberwarfare under Article 51.

1. Can Cyberwarfare Constitute an "Armed Attack" Under Article 51?

Much like "breach of peace" and "use of force," the U.N. has not presented a definition or set of guidelines regarding what type of state action is considered to be an "armed attack." Scholars have offered different approaches to determining whether or not a cyber attack could constitute an "armed attack" under Article 51 of the Charter. What complicates this

52. U.N. Charter art. 51. ("Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.").

53. Jensen, *supra* note 30, at 218 ("Though at times the doctrine has been used to justify aggressive actions, self-defense has been enshrined as a legitimate principle of international law and was included in the U.N. Charter precisely because the founding delegates mistrusted complete reliance on collective security.").

analysis when looking to the U.N. Charter is the fact that cyberwarfare could not have been considered by the drafters, as well as the fact that cyberattacks are not easily compared with traditional forms of warfare under this framework.[54]

Within this ambiguous and unchartered legal analysis, the International Court of Justice (ICJ) has previously considered what types of actions could be classified as an "armed attack," for example in Nicaragua v. United States.[55] In this case, the ICJ considered whether or not U.S. actions of intervention fell under Article 2(4)'s prohibition on improper uses of force.[56] The U.S. alleged that in supporting the Contras in Honduras against Nicaragua, it was intervening on behalf of Honduras' right to self-defense.[57] The ICJ considered the U.S.'s funding and supplying weapons as an improper use of force, as Nicaragua's actions fell short of an "armed attack."[58] The ICJ held that a "use of force" under Article 2(4) is not always considered to be an "armed attack," and that a mere intervention by one state into another dispute between nations does not always constitute a "use of force" as prohibited by the Charter.[59] While the ICJ didn't offer much clarification for the standard, their findings are still illuminating. Under this analysis, it appears that even some degree of military action could fall short of a "use of force" within the Charter, and additionally, the ICJ implicitly decided that an "armed attack" is a higher threshold than a "use of force" under Article 2(4).

From this analysis by the ICJ, acts of aggression in the cyberwarfare context under current international law seem that they would fall comfortably below the threshold of "armed" force.[60] By not establishing a clear definition of what actions would cross this threshold, the international community has opened the door for nations to exert as much force as they would like in the cyber world, without having to worry about retaliation under Article 51. Because the advancements of warfare and influence have evolved much faster than the accompanying legal doctrine designed to keep international aggression and force in check, unless the U.N. addresses this problem in the near future, these conditions are likely to fuel an arms race like that of the Cold War. The only difference is that in the cyber context, this

54. MELZER, *supra* note 1, at 9 ("The truth is that cyber operations, almost always falling within the grey zone between traditional military force and other forms of coercion, simply were not anticipated by the drafters of the UN Charter and, so far, neither state practice nor international jurisprudence provide clear criteria regarding the threshold at which cyber operations not causing death, injury or destruction must be regarded as prohibited under article 2(4) of the UN Charter.").

55. *See generally* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27) ("There appears now to be general agreement on the nature of the acts which can be treated as constituting armed attacks.").

56. Jensen, *supra* note 30, at 219.

57. *Id.*

58. *Id.*

59. *Id.*

60. Dever & Dever, *supra* note 45, at 35 ("[U]nder the current framework cyberattacks would very rarely constitute an armed attack or even an act of aggression because they do not appear to cross the ICJ's admittedly less than clear threshold of use of force or aggression, and because they do not usually involve armed forces in the conventional senses, and because it is difficult to make an analogy between cyberattacks that do not actually involve the use of weapons, and conventional acts that involve armed forces.").

will be much harder to monitor and control, as many more players will be involved and the consequences of new tactics have yet to be understood. Since the current framework has yet to be challenged by a cyberattack coming close to an "armed attack," looking to different approaches suggested by scholars will shed light on how cyberattacks may be analyzed under Article 51 if and when such an attack occurs.

a. Instrument or Method-Based Approach

One approach to analyzing whether an "armed attack" has occurred, rests this distinction on whether or not the cyberattack was executed in conjunction with a traditional military operation, focusing on the instruments used to conduct an attack.[61] This approach looks to the method in which the attack was carried out, which would consider traditional kinetic methods of war to be the focus of analysis under Article 51. One shortcoming of this approach is that it seems to be grossly under-inclusive and ignorant to the potential effects of an attack, looking only to the instrument or method of how the attack was carried out. Under this analysis, a nation using sophisticated cyberweapons could cause any damage imaginable to another country, and as long as it never fired a bullet or dropped a bomb, it would seem to be sheltered by the U.N. Charter from any retaliatory strike from the attacked nation.

There is however some degree of support for this view in the language of the U.N. Charter, and some scholars point to this textual support to strengthen this argument.[62] Under Article 41 of the Charter, discussing potential actions of the Security Council in the event of a "breach of peace" as mentioned above, the language classifies various different methods including "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication . . . ."[63] This article specifically classifies these methods as "measures not involving the use of armed force," suggesting that if such methods were instead used by an aggressor during an attack, this would not constitute "armed force" and would not warrant a nation's right to self-defense under the Charter.[64] While this language is very precise and clear, and may in fact validly exclude certain types of cyberattacks like distributed denials of service and other minimally damaging network compromises, there are certainly other types

61. Hathaway et al., *supra* note 22, at 845-46 ("[A] cyber-attack alone will almost never constitute an armed attack for purposes of Article 51 'because it lacks the physical characteristics traditionally associated with military coercion'—in other words, because it generally does not use traditional military weapons. This approach treats a cyber-attack as an armed attack only if it uses military weapons."). Hathaway characterizes this approach as an "instrument-based approach." *Id.* at 845.

62. *See id.*; *see also* MELZER, *supra* note 1 at 7 ("The *travaux préparatoires* of the UN Charter clearly show that the prohibition of 'force' was not intended to extend to economic coercion and political pressures. Also, article 41 of the UN Charter refers to 'interruption of . . . communication' as a 'measure not involving armed force', thus suggesting that certain denial of service attacks (DOS) would not fall under the prohibition of article 2(4).").

63. U.N. Charter art. 41.

64. *Id.*

of cyberwarfare that may be so damaging that a state might be warranted in responding under self-defense.[65]

By looking only to the instrumentality of an attack, this approach could create exclusions for all kinds of attacks as long as traditional military methods are not employed. Consider for example the possibility of biological warfare waged against another nation. If a chemically engineered virus was unleashed against another nation, killing thousands of people, a strict application of this approach would likely yield an improper answer to the question of whether or not self-defense should be legally justified, since the attack lacked the instrumentality of traditional combat. When considered in this light, it does not make sense that the Charter would be so focused on the means of an attack, that it would discourage a nation's right to self defense even if the actual effects of the attack were equivalent to those of a traditional military attack.[66]

The instrument-based approach puts far too much emphasis on the means by which an attack is carried out, without sufficient consideration for other critical factors like the tangible consequences of an attack or the intent and importance of the target for the attack. While this analysis is likely the most straightforward and easily measurable, its shortcomings make it an inadequate framework within the evolving world of cyberwarfare.

b. Target-Based Approach

Other scholars have considered a determination of an armed attack based upon the significance of the resources or networks targeted by the cyberattack.[67] This target-based approach addresses attacks that are focused on critical networks or infrastructure, and would allow states to respond militarily if a cyberattack was directed at a network meeting a certain threshold of importance. Analyzing this issue with due regard to the target is an important consideration, as it would limit instances of cyberattacks causing mere inconvenience, and would look instead to those which likely had more nefarious intentions.

By looking toward the target, nations could easily draw a distinction to determine which critical infrastructures would warrant a response when compromised by a cyberattack from another nation. However, one important criticism of this approach is that it is focuses too much on the target, without due focus on the actual damage or effects of the cyberattack.[68] While the

65. *See* Hathway, *supra* note 22, at 846 ("The chief advantage of the instrument-based approach is simplicity of application, since uses of military weapons and force are relatively easy to identify. However, because cyber-attacks have the potential to cause catastrophic harm without employing traditional military weapons, most scholars have rejected the instrument-based approach to defining armed attacks as dangerously outdated.").

66. MELZER, *supra* note 1, at 8 ("[T]he Charter cannot allow that the prohibition of interstate force be circumvented by the application of non-violent means and methods which, for all intents and purposes, are equivalent to a breach of the peace between the involved states. Consider, for example the crippling effect of cyber operations disabling the electrical power grids of major cities, the incapacitation of systems controlling industrial production, or the infiltration of malware designed to "blind" an entire air defence system.").

67. Hollis, *supra* note 26, at 1041; *see* Hathaway et al., *supra* note 22, at 32.

68. Hollis, *supra* note 26, at 1041 ("[T]he 'target-based' approach suggests [a cyberattack] constitutes a use of force or an armed attack whenever it penetrates 'critical national infrastructure' systems, even absent significant destruction or casualties.").

previous approach left room for under-inclusion, the target-based approach may be over-inclusive. Here, a state could respond with military strikes against the aggressor country, even if the cyberattack was minimally effective or damaging. This approach treats all cyberattacks as essentially the same in terms of severity, focusing instead on the nature of the target exclusively without considering whether a military strike would be reasonable under the circumstances. Taken to an extreme example, Russian hackers have allegedly been behind countless cyberattacks directed at U.S. diplomats and the State Department, and have even acquired significant amounts of data including Obama's personal itineraries and correspondence, but it is highly unlikely that the U.S. would be justified in sending troops to Russia because the target of the hack was highly important.[69]

Part of the problem of this approach is that it almost encourages over-reactions by states that have found themselves on the receiving end of a cyberattack targeting a critical network, as the state would be legally justified in taking military measures out of anticipatory self-defense to ensure a serious breach does not occur again.[70] This standard would likely promote escalation instead of discouraging it, and it would push states closer to fighting a traditional war when their networks are targeted, because there would be a lower threshold for legal authorization of force under the U.N. Charter.[71]

c. Effects-Based Approach

Likely the most practical method in determining whether a cyberattack constitutes an "armed attack" would be to look not exclusively at the target or the instrument of the attack like the former approaches, but instead to the tangible results and consequences of the cyberattack.[72] This analysis seeks to address some of the issues with the former two, to reduce over and under-inclusion while attempting to create a clear doctrine for application in this new form of warfare. A significant problem with this approach is that scholars disagree over what threshold the effects of the attack must pass in order to be classified as an "armed attack" within the meaning of Article 51.

69. *See, e.g.*, Paletta, *supra* note 5 ("Russian hackers have targeted diplomatic and political data, burrowing inside unclassified networks at the Pentagon, State Department and White House, also using emails laced with malware, according to security researchers and U.S. officials. They have stolen President Barack Obama's daily schedule and diplomatic correspondence sent across the State Department's unclassified network, according to people briefed on the investigation.").

70. *See* Hathaway et al., *supra* note 22, at 846.

71. *Id.* at 846-47. ("While the target-based approach has the benefit of allowing for aggressive protection of critical national systems, it broadly sanctions forceful self-defense, increasing the likelihood that cyber-conflicts will escalate into more destructive conventional armed conflicts. . . . This approach could undermine the security of the international community by making war much more likely.").

72. *See* Hathaway et al., *supra* note 22, at 847 ("[T]he effects-based approach classifies a cyber-attack as an armed attack based on the gravity of its effects. Steering a middle course between the instrument- and target-based views, the effects-based approach is the most promising and most widely accepted approach."); MELZER, *supra* note 1, at 14; *see also* Hollis, *supra* note 26, at 1041 ("[T]he 'consequentiality' approach, favored by the U.S. Department of Defense, focuses on [cyberattack] consequences; whenever [a cyberattack] intends to cause effects equivalent to those produced by kinetic force (death or destruction of property), it constitutes a use of force and an armed attack.").

One method of analysis sets this threshold at the level of physical destruction and casualties representative of a traditional military attack.[73] An issue with this standard is that it creates an exclusion for any cyberattacks that do not have a physical element to them.[74] While this reasoning would rightly justify retaliation in situations when many lives are lost and physical damage is substantial, it overlooks instances when there could be still be significant damage and harm albeit lacking the concrete elements of physical destruction and death needed to satisfy the threshold. For example, if a cyberattack completely shut down the stock market or created a nation-wide power outage, the harm to the U.S. would be incredibly high and indicative of damage that could occur in traditional warfare, but without the physical elements, this standard would not be met and the U.S. would not be justified in retaliating.

A more comprehensive analysis would also include consideration of situations where mass casualties are not present, but significant damage or interruption of important infrastructure networks has resulted.[75] However, such considerations must be weighed carefully, as there is no clear and easy method of drawing the line where death and physical damage are absent, but economic or infrastructure compromise has been substantial.[76] The effects-based approach has also been challenged because it might open the door to include economic coercion, as harsh sanctions against a country may ultimately have similar effects as cyberattacks targeting critical computer networks.[77]

Michael Schmitt, a leading scholar and supporter of the effects-based approach, has argued that the effects of a cyberattack should be analyzed according to six different factors when determining whether it should amount to an "armed attack" under Article 51.[78] These factors include: (1) severity: the type and scale of the harm; (2) immediacy: how quickly the harm materializes after the attack; (3) directness: the length of the causal chain between the attack and the harm; (4) invasiveness: the degree to which the attack penetrates the victim state's territory; (5) measurability: the degree to which the harm can be quantified; and (6) presumptive legitimacy: the

73. *See* MELZER, *supra* note 1, at 14.

74. *See* Richardson, *supra* note 11, at 13 ("Given the unique nature of cyber attacks, as distinguished from kinetic or conventional weapons-based attacks, damage or destruction in the traditional sense is often minimal. However, the more significant harm rendered by a cyber attack takes the form of significant disruption (but not permanent destruction) to computer controlled systems, including online banking, electrical grids, telephone systems, and the like.").

75. *See id.* at 16; *see also* Hathaway et al., *supra* note 22, at 35.

76. *See* MELZER, *supra* note 1, at 14 ("The main problem is that, depending on what is considered to be 'equivalent' to physical destruction, this approach will either end up being too restrictive (that is, including only cyber operations directly resulting in physical destruction but not, for example, the 'mere' incapacitation of the entire national power grid, telecommunication network or air defence system) or too expansive (that is, including any large-scale denial of service attack even against non-essential, civilian service providers . . .).").

77. Jason Barkham, *Information Warfare and International Law on the Use of Force*, 34 N.Y.U. J. INT'L L. & POL. 57, 86 (2001) (Barkham criticizes a broad effects-test, stating that such an approach "would blur the distinction that excludes economic coercion from the use of force. . . . Economic sanctions, for example, can have the same effects over long periods of time as missile attacks aimed at infrastructure targets. . . . If the use of force analysis relies on the result-oriented approach, there may be no meaningful way to exclude economic acts.").

78. Hathaway et al., *supra* note 22, at 847.

weight given to the fact that, in the field of cyber-activities as a whole, cyber-attacks constituting an armed attack are the exception rather than the rule.[79] These factors are important to consider when diagnosing the severity of an attack, and at minimum can help set a framework for analyzing the vast spectrum of cyberattacks as they relate to a nation's right to self-defense under Article 51. Schmitt's six-factor test has been criticized[80] by other scholars for not effectively analyzing the issue and being impractical in the event of an actual emergency situation, but many scholars tend to lean towards the effects-based approach in general for its analytical and practical considerations.

Another example of an analytical framework under the effects test has been promoted by Daniel Silver, a former attorney of the National Security Agency and Central Intelligence Agency. Silver has argued that Schmitt's six-factor test could be analyzed to include virtually any cyberattack as a use of "armed force" under Article 51 and claimed that a more straightforward approach would more adequately pave the way for analyzing an attack.[81] He further argues that the most critical elements to consider when diagnosing a cyberattack are severity and foreseeability.[82] Accordingly, a cyberattack will cross the line of "armed force" and grant a nation legal justification for self-defense "only if its foreseeable consequence is to cause physical injury or property damage and even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion."[83] This recommendation of an effects-based approach seems to be a much less complicated than that of Schmitt's, and could more easily be analyzed in the wake of a cyberattack. One potential shortcoming of this approach however, is the consideration of foreseeability. While this element is important to consider, it seems that at a certain threshold of severity of harm, it isn't likely to matter what the foreseeability was at the time.[84] If a nation sought to conduct espionage and hack a government agency, and instead caused a nuclear meltdown and harmed thousands of civilians, it is unlikely that a country like the U.S. would rule out retaliation based on the lack of foreseeability of the actual harm. In this sense, while foreseeability may be included in the analysis, severity of harm should be the critical element in the framework.

---

79. *Id.*

80. Barkham, *supra* note 77, at 85–86 ("In effect, Schmitt's approach is backwards, because it requires determining the legitimacy of an attack under international law (i.e., distinguishing between acts of coercion and uses of force) by asking whether the attack is legitimate. . . . IW attacks cannot be assessed readily at the time of the attack to determine their magnitude and the permitted responses. This problem will arise with any framework that requires an ex post analysis. The difficulty of tracing IW attacks will undermine severely any state's willingness to wait out the attack before responding because its best opportunity to respond effectively occurs if it detects the attack in progress and responds immediately.").

81. Hathaway et al., *supra* note 22, at 848.

82. *Id.*

83. *Id*.

84. *Id.* (quoting Daniel Silver's opinion that cyber-attack self-defense is only justifiable "if its foreseeable consequence is to cause physical injury or property damage . . . ."). Under Silver's recitation of the effects test, "a cyber-attack on the air traffic control system causing planes to crash would be regarded as an armed attack because it is foreseeable that such an attack would cause loss of life and substantial property damage. But a cyber-attack on a website or mere penetration of a critical computer system generally would not, unless it caused physical injury or property damage." *Id.*

Among the three perspectives outlined above, the effects-based approach seems to be the most practical in adapting cyberwarfare to Article 51 and giving nations a usable framework in analyzing the gravity of a cyberattack as it relates to the right of self-defense under the U.N. Charter.[85]

2. Anticipatory Self-Defense under Article 51?

Beyond the issue of how to determine whether or not an "armed attack" has occurred under Article 51, lies the pressing subsequent issue of whether or not a state may respond in anticipatory self-defense toward an imminent threat.[86] This consideration is particularly relevant in the cyberwarfare context due to the nature of cyberattacks. It is often incredibly difficult to diagnose the severity of an attack once a breach has occurred, and a nation may either disregard or overreact to a breach of their network, not knowing if further attacks (either kinetic or cyber) are going to come shortly after the initial attack. Many cyberattacks that occur are considered "probing" attacks, designed to find weaknesses in computer networks, but not necessarily intended to cause catastrophic harm.[87]

Outside the realm of cyberattacks, there has been considerable debate among scholars regarding a state's right to anticipatory self-defense. Some scholars have argued for an extremely strict application of Article 51, proposing that a state is not entitled to self-defense unless and until it has tangibly suffered an "armed attack," and regardless of the state's speculation or anticipation of an impending attack, there is no legal justification for a retaliation until the initial attack has occurred.[88] Other scholars have argued for a much more lenient standard in extending Article 51 to anticipatory self-defense, claiming that under certain circumstances, such anticipatory actions are not only justified by logic, but also historical analysis under international law.[89] These scholars point to a legal doctrine called the *Caroline* test, in which the question of anticipatory self-defense was analyzed long before the adoption of the U.N. Charter.[90] Under this test, a nation would be justified in responding with anticipatory force when the "necessity of that self-defense is instant, overwhelming and leav[es] no choice of means, and no moment for deliberation."[91]

85. *See* MELZER, *supra* note 1, at 26 (arguing that "acts of violence" include those non-kinetic actions whose effects cause "physical destruction of objects," injury, and/or death).

86. Dever & Dever, *supra* note 45, at 37 ("The term 'anticipatory self-defense' in the context of international law and *jus ad bellum* is commonly defined as a nation's ability to foresee the consequences of a given threat and to take proactive measures aimed at preventing those consequences. Accordingly, anticipatory self-defense is distinguished from armed reprisal in that the former is protective while the latter is retributive.").

87. *Id.* (arguing that if anticipatory self-defense is to be allowed within the cyberwarfare context, then "[m]uch more attention would have to be paid to the concept of 'probing' attacks, and whether such activity amounts to small scale attacks that may be compiled together and responded to with greater force").

88. Hoisington, *supra* note 19, at 449–50.

89. *See id.* at 450.

90. *Id.*

91. *Id.* ("Legal scholars supporting the latter stance argue that article 51 incorporates customary international law as articulated by the *Caroline* standard, allowing anticipatory self-defense. As defined by then Secretary of State, Daniel Webster in the *Caroline* case, this point in time occurs when the

Michael Schmitt has proposed a framework for justifying anticipatory self-defense only if three important factors are met.[92] Schmitt argues that in order for an anticipatory strike to be justified, the cyberattack must (1) be a part of a larger attack, likely to be followed by "armed force"; (2) the cyber attack is an "irrevocable step" towards an imminent attack; and (3) "[t]he defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack."[93] Schmitt's test doesn't offer any clarification on how those factors could realistically be diagnosed in the midst of an unfolding cyberattack, but the consideration is still relevant when asking when anticipatory strikes should be considered. Under this analysis, it is difficult to consider how one would be able to quickly analyze a cyberattack along such parameters, but it is likely that in some rare cases, if the cyberattack was sufficiently threatening, anticipatory self-defense could be justified.

C. COMPLICATIONS WITH APPLYING CYBERWARFARE TO THE CURRENT CHARTER: ATTRIBUTION, INTENT, AND DISTINGUISHING TARGETS

For various different reasons, cyberwarfare is incredibly difficult to analyze under Article 51 because it lacks many qualities of traditional warfare, which the article was originally created to address. One significant issue that distinguishes cyberattacks from traditional warfare is the inherently high likelihood for accidents.[94] As discussed previously, many nations engage in cyber-reconnaissance and infiltrate networks to access data, and this has yet to be characterized as an act of cyberwarfare among the international community. However, once an infiltrator has breached a network, it is likely that while trying to access information, substantial damage could occur accidently. An example of this allegedly occurred in 2012, when Syria's internet was shut down accidently when some unknown actor was trying to access protected information.[95] Another example for consideration is Stuxnet. Plenty of things could have gone wrong with this cyberattack, and while it was considered an attack of deterrence, it is unlikely that the Iranians would have agreed with that characterization if the attack had caused a nuclear meltdown in one of their facilities. It was discovered that the Stuxnet worm actually ended up spreading to other computers around the world that were not intended to be targets of the attack, and it

'necessity of that self-defence is instant, overwhelming and leaving no choice of means, and no moment for deliberation.'").

92. Jensen, *supra* note 30, at 225.

93. *Id.* ("Schmitt also advocates anticipatory self-defense, but only if three factors are present: (1) The CNA is part of an overall operation culminating in armed attack; (2) The CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack; and (3) The defender is reacting in advance of the attack itself during the last possible window of opportunity available to effectively counter the attack.").

94. *See* Sebenius, *supra* note 4.

95. *Id.* ("Edward Snowden tells us that this was not an intentional attack against the Syrian internet but this was a case of someone trying to do espionage and inadvertently making a mistake and causing an outage to the internet.").

would have been a diplomatic nightmare if this worm ended up spreading to one of our allies and causing damage.[96]

This propensity for accidents and virus proliferation creates a dilemma because not only is it likely that accidents may happen without intent, but also that actors deliberately intending the damage could hide behind this likelihood as an excuse to avoid military confrontation, arguing that they were simply intending espionage and not a substantial cyberattack.[97] This complicates things from a legal analysis perspective as well, because it may eliminate "intent" from being considered at all when weighing a response to such attacks.

The more complicated issue with cyberattacks involves attribution and responding to the correct party responsible. Unlike most instances of conventional warfare, a cyberattack does not always leave a clear path of blame to the instigator. Because of the nature and accessibility of cyber networks, a hacker with no state affiliation could cause significant damage and compromise critical infrastructures and secure networks of another nation's private sector or government network. While a state may be justified in defending itself in response to an attack by another nation, the consideration is blurred when the attacker is an actor unaffiliated with a state.[98] It is unclear whether or not a state could invoke self-defense against another nation after suffering a cyberattack from one of its citizens, especially if the actor was operating completely independent from the nation, or further, how a nation might respond directly to the threat in distinguishing and targeting the actors responsible.[99]

---

96. T.S., *A Cyber-Missile Aimed at Iran?*, ECONOMIST: BABBAGE (Sept. 24, 2010), https://www.economist.com/babbage/2010/09/24/a-cyber-missile-aimed-at-iran ("Microsoft said in August that more than 45,000 computers around the world had been infected by Stuxnet. An analysis by Symantec, a computer- security firm, found that 60% of infected machines were in Iran, 18% in Indonesia and 8% in India."); Richardson, *supra* note 11, at 5 ("Stuxnet was originally detected in early 2010 by a computer security company in Belarus, and subsequently found to have infected (albeit without causing much actual harm) thousands of industrial control systems world-wide.").

97. *See* Sebenius, *supra* note 4 ("[T]his makes any intrusion into a foreign network more threatening or seem more threatening, because even if the intentions of the intruder are not to cause damage, it might inadvertently do so.").

98. Hathaway et al., *supra* note 22, at 845 n.111 ("Once a state has been the victim of an armed attack, a further question arises as to against whom the state can respond. Where the armed attack is perpetrated by a state, this question is easily answered—self-defense may be directed against the perpetrating state. However, cyber-attacks may be perpetrated by non-state actors or by actors with unclear affiliations with state security agencies.").

99. *See id.* ("Although some scholars argue that cyber-attacks (and conventional attacks) must be attributable to a perpetrating state in order for the victim state to take defensive action that breaches another state's territory, others—drawing on traditional jurisprudence on self-defense—argue that states possess the right to engage in self-defense directly against non-state actors if certain conditions are met."); *see also* MELZER, *supra* note 1, at 10 ("Persons or entities who are not acting on behalf of a state or whose link to a given state is insufficient to engage its international legal responsibility, on the other hand, cannot be regarded as state agents and can be described as 'non-state actors'. . . . The use of force (including through cyber operations) by individual hackers and other non-state actors may be relevant under international humanitarian law and, in some cases, international criminal law, but is not prohibited by article 2(4) of the UN Charter."); *id.* at 5 ("While cyberspace is readily accessible to governments, non-state organizations, private enterprises and individuals alike, IP spoofing and the use of botnets, for example, make it easy to disguise the origin of an operation, thus rendering the reliable identification and attribution of cyber activities particularly difficult.").

This issue of attribution is further complicated by the fact that it is incredibly difficult to trace a complex cyberattack to the guilty party, and some attacks even create a false path to a network uninvolved in the operation.[100] If a nation was crippled by a cyberattack, and a diagnostic test shows that the attack came from another nation who thereafter denies responsibility, how must the nation respond? This hypothetical illustrates the serious issue of attribution and how complicated it can become to find the correct party to retaliate against, especially considering the potential for anonymity of attacks from an encrypted source. Attributing blame to the correct perpetrator is incredibly important because the application of Article 51 requires that self-defense measures be taken in response to an attack by a country or an agent of the country. If this line of agency connection is unclear, it is unlikely that a nation would be legally justified in taking defensive action.[101] Without being able to confidently attribute at attack to a perpetrator, granting nations the right to self-defense after such an attack could be incredibly problematic. Unlike a kinetic attack against a nation, determining the source, intent, and affiliation of cyberattack perpetrators is nearly impossible to do with any degree of certainty within a short period of time, and this poses a significant problem when weighing strategic options for retaliation.[102]

These difficulties are particularly important because in order for a nation to be able to exercise this right of self-defense, the actual response has to meet some important criteria.[103] These criteria are necessity, proportionality, and immediacy.[104] In order to diagnose necessity, a nation "must attribute the attack to a specific source, characterize the intent behind the attack, and conclude that the state must use force in response."[105] In meeting the standard for proportionality, the retaliation must be directly proportional in force to the attack initially suffered by the state.[106] Immediacy requires that a retaliatory response must occur within a reasonable amount of time from the initial attack.[107] As discussed previously, in the cyberwarfare realm, none of these factors under "necessity" are easily distinguished, and determining them would be incredibly burdensome and time-consuming. Similarly, the proportionality prong would be very difficult to meet as well. While one could argue that mimicking the type of cyberattack suffered would be

100. *See* Shackelford, *supra* note 15, at 231 ("The problem then becomes one of attribution, that is, the all too familiar scenario of computer systems being used maliciously without the knowledge of the network administrator. For example, many of the 'zombie' computers used to carry out botnet attacks against Estonia turned out to be in the U.S. Should Estonia then have a right of self-defense against the U.S.?").

101. *See* Hoisington, *supra* note 19, at 451.

102. Jensen, *supra* note 30, at 232 n.153 ("Understanding the distinctions between attacks and motives, and improving our nation's ability to provide fast and accurate assessments of the nature of both the attacks and their perpetrators, are a core part of the problem at hand. [B]oth the likely criminal entities and the damage they seek to inflict become more difficult to identify, quantify, and warn against. It is increasingly complicated to distinguish between a national security threat, criminal activity, and malicious but low-level disruption.").

103. *See* Hoisington, *supra* note 19, at 450.

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

proportional, this does not consider instances when a nation might not have the same capabilities as the aggressor in the cyber context, and instead wishes to respond militarily. It is unclear whether or not a military response could be considered "proportional" unless catastrophic damage was suffered by the initial attack, making this current framework incredibly inflexible when looking at a nation's justifiable responses.

These differences between cyberwarfare and traditional combat illustrate why the legal analysis under the U.N. Charter can be incredibly difficult when diagnosing an attack occurring across computer networks instead of tangible borders. This Charter was not written to address this new type of conflict, and the U.N. must take steps to make its application up to date with current technology and the unique elements of cyberwarfare.

IV. CONCLUSION

It is clear that international law has not quite kept up with the needs of an evolving technological landscape and the potential for nefarious activity within that forum. While it is prudent that the international community address these issues directly, for now there should at least be a dialogue about how a nation may determine its rights to engage and retaliate if it suffers a severe cyberattack. The legal analysis under Article 51 could be improved and clarified by creating a hybrid analysis, consolidating certain elements of the "target-based" and "consequence/effect" approaches, so that the U.N. can establish an effective test to determine whether or not an "armed attack" has occurred.[108] In this sense, a cyberattack would be measured primarily on the tangible effects suffered, but these would not necessarily be limited only to deaths or physical damages. In the event that those harms were absent, but a significant "target" or critical infrastructure[109] network was substantially impaired, states would have justification in retaliating against the perpetrators of the attack.

While this test is not without flaws, it is important to have some kind of doctrine to refer to in the event that a catastrophic cyberattack occurs, and the U.N. should take responsibility in clarifying how this analysis should be executed. Having a foundation in place is critically important when responding to a crisis, otherwise, the first country to suffer a crippling cyberattack may take matters into its own hands and set a precedent of rogue action due to the ambiguity in the current legal doctrine under the U.N. Charter.[110]

Nations must come together to determine which actions are acceptable and unacceptable in the realm of cyberwarfare, much like they did with traditional combat after World War I in relation to chemical weapons. If this blurred area of sabotage and espionage is not clarified soon, it is only a matter of time before one nation makes a decision to unleash a devastating

108. *See* Hathaway et al., *supra* note 22, at 847.

109. *See* MELZER, *supra* note 1, at 15 ("[T]he term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.").

110. *See* Dever & Dever, *supra* note 45, at 33.

cyberattack under unclear legal rules. While it may be incredibly difficult and controversial to draw a line on this issue, if cyberwarfare as it relates to the U.N. Charter is not addressed in the near future, it could easily spur the next global military conflict. Ambiguity regarding consequences for state action does not lead powerful nations to stand by idly, but rather escalate their capabilities and take advantage of this unchartered territory. The U.N. should not wait for World War III to unfold before deciding to address a situation that has been proliferating and gaining momentum over the last two decades, but should instead face the challenge and define clear standards and a relevant legal doctrine before this procrastination presents serious consequences.