Cyber Warfare and International Law: The Need for Clarity

Cameron H. Bell*

Abstract: *The internet and computerization have revolutionized how humans and states interact. However, with these new technologies comes a new arena for conflict between states. The definition of aggression under U.N. General Assembly Resolution 3314 is inadequate in addressing these new threats. This work suggests the addition of an inclusive definition of cyber warfare to the current internationally accepted definition of aggression. Additionally, through analysis of cyber-attacks on Estonia, Georgia, Iran, the Philippines, and the United States, this work will show that while cyber-attacks violate international law under Resolution 2625, and should be considered acts of aggression, the language of Resolution 3314 is such that these attacks do not meet the current legal definition of aggression. Moreover, this analysis will show that, through the use of cyber weapons, states have successfully circumvented Resolution 3314, allowing aggressor states to take destabilizing actions with near impunity.*

Introduction

The advent of the internet and computerization is a great leap forward for humanity. These new technologies aid in everything from communication to education to medicine. However, as technology and the internet have spread into almost every facet of daily life, both in the civilian sector and the military and defense sectors, these advancements open the world to a new arena for conflict. The ongoing global cyber arms race and the use of these new weapons of war threaten global stability. Within the last decade there has been a marked increase in state-sponsored cyber-attacks both in the civilian and governmental sectors. This increase marks a change in how states perceive and use cyber weapons, creating an opportunity for conflict where previously none existed.[1] Some international organizations, such as NATO (North Atlantic Treaty Organization), have attempted to address this new potential for conflict through works such as the Tallinn Manual, a guide to cyber warfare and accepted responses developed in response to the 2007 Russian cyber-attacks on Tallinn, Estonia. However, these attempts have not kept up with the pace of technological advancement, which has been too rapid for the international system to develop a clear and adequate response. The 2007 cyber-attacks on Estonia, the use of cyber weapons in Georgia in 2008, the U.S. cyber-attack against Iran in 2008-2009, and the more current use of cyber weapons for information warfare by countries such as Vietnam, and by Russia in the 2016 U.S. election provide case studies to show the range of

*Cameron H. Bell is an undergraduate student at Towson University in Baltimore, Maryland. Upon graduating he will receive Bachelor's Degrees in History and Asian Studies.

[1] Benjamin Jensen, Brandon Valeriano and Ryan C. Maness. "Cyberwarfare has taken a new turn. Yes, it's time to worry," *The Washington Post*. July 13, 2017. https://www.washingtonpost.com/news/monkey-age/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/?utm_term=.41b9f74519ec Accessed February 15, 2018.

weapons now in use, as each attack used vastly different methods. Furthermore, the vast differences in each attack shows why providing a clear and precise definition of cyber warfare is a complicated, but imperative task.

There is an ongoing debate within the international and academic communities on whether cyber-attacks constitute use of force and are acts of aggression under the current U.N. Resolution 3314: Definition of Aggression. This debate can be seen through the respective works of Nils Melzer and Priyanka Dev: "Cyber Warfare and International Law" written in 2011, and "'Use of Force' and 'Armed Attack' Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response" written in 2015.[2] The U.N. General Assembly Resolution used to define aggression and use of force, Resolution 3314: Definition of Aggression, was created in 1974 prior to the advent of the internet and the integrated computer systems in use today. The Definition of Aggression Resolution was designed to clarify which actions states may not take against each other; however, since it was written before the internet, the language used in this Resolution does not clearly incorporate cyber weapons. In the ongoing debate, I contend that cyber-attacks are acts of aggression and do violate Resolution 3314 in spirit, but not in its explicit language. This absence of clear language, explicitly including cyber-attacks, in the definition of aggression has created a gray area in which states feel they can use these weapons without their actions being labeled as aggression. An additional Resolution according to which these attacks may be understood as being in violation of international law, is Resolution 2625, the "Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nations." The 'Friendly Relations' Resolution, introduced in 1970, outlines acceptable conduct of member states in their interactions. These two Resolutions will be used to show that cyber-attacks are clear violations of international law; however, the lack of an explicit cyber component in the Definition of Aggression Resolution has created a grey area, which some states may consider a loophole, allowing the use of cyber weapons. Analysis of recent cyber-attacks using these two U.N. Resolutions will show that cyber-attacks draw into sharp relief that states can act in an unfriendly manner without their actions being labelled as acts of aggression.

Finally, given the difficulty in defining cyber weapons and the failure of Resolution 3314 to adequately address cyber warfare, states that have been subjected to such attacks should be able to respond in kind without fear of judgement or retaliation from the international community until international organizations, such as the U.N., develop and enact new definitions and laws specific to cyber warfare and the right of retaliation or compensation of affected states. Cyber-attacks are in violation of international law, specifically U.N. General Assembly Resolution 2625; however, due to the lack of explicit language relating to cyber warfare in the U.N. definition of aggression in General Assembly Resolution 3314, cyber weapons are currently being used without being labelled acts of aggression. Furthermore, while Resolution 2625 outlines the principles of international law concerning "friendly relations and cooperation among states," it does not discuss actions of aggression which states may use as a reason for war under international law. In contrast to the 'Friendly Relations' Resolution 2625, the 'Definition of Aggression' Resolution 3314 defines what constitutes an act of aggression under the U.N.

[2] Nils Melzer, "Cyber Warfare and International Law," United Nations Institute for Disarmament Research. United Nations. 2011.; Priyanka Dev, ""Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," *Texas International Law Journal* Vol. 50 Issue 2 (Spring 2015) p379-399.

Charter. Thus, on the discussion of cyber warfare, a violation of Resolution 3314 holds more importance for state actions and international stability than a violation of Resolution 2625. However, 'Definition of Aggression' lists seven general scenarios, which are considered acts of aggression, with each scenario entailing physical armed force or physical action by a state, such as the bombardment of cities, invasion of territory by armed forces, or the blockading of ports. The physical nature of this resolution has led many to conclude that cyber-attacks do not meet the physical requirements listed in the Resolution, nor do they constitute armed force under Resolution 3314.[3] International law must meet reality; reality cannot be forced to meet existing law. Therefore, to resolve any confusion with Resolution 3314, there should be a cyber warfare component added to the definition of aggression. This will enable states to act with surety when harmed by cyber weapons, and it will stabilize the currently unstable environment which the international community is operating in.

Current International Cyber Laws

The current international legal system is built on principles which themselves are formed through customary practice by states. A customary practice, in the international legal sense, according to J.L. Brierly, "means something more than mere habit or usage; it is a usage felt by those who follow it to be an obligatory one. There must be present a feeling that, if the usage is departed from, some form of sanction will probably, or at any rate ought to, fall on the transgressor."[4] After a customary practice is identified and accepted by U.N. member states, it is drafted into written international law through treaties or U.N. resolutions.[5] However, it is important to understand that international law does not function like domestic law and there are no guaranteed, but only expected, consequences for violating international law. Moreover, states must consent to being subject to an international law. According to J.L. Brierly, international law is not meant to provide concrete solutions to specific problems, rather it is meant to create structures for understanding state conduct and actions, and provide a framework for response.[6] Through the use of international law, states are able to identify issues, such as acts of aggression, and understand the internationally accepted response options available to them. This creates a more stable environment in which states can interact in an understandable and predictable fashion.[7]

Crafting international law is a slow process because it entails the formation of consensus among states prior to the acceptance of a general practice as law, thereby making the process ill-suited to responding quickly to fast-developing technologies such as cyberspace. Existing international law on internet and computer technology has remained largely focused on international trade law and trademark law. While there are robust laws and practices regarding private, individual use of the internet, there is almost no precedent or customary practices

[3] Chance Cammack, "The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression," *Tulane Journal of International and Comparative Law*, Vol: 20, 2011/01/01. p. 306, 322.

[4] J.L. Brierly, *The Law of Nations: An Introduction to the International Law of Peace.* (Oxford: Oxford University Press, 1963). p. 59.

[5] Anthony Clark Arend, "International Law and the Preemptive use of Military Force," *The Washington Quarterly* 26:2, Spring 2003. p. 90.

[6] J.L. Brierly, *The Law of Nations.* p. 76.

[7] Ibid. p. 77-78.

established to address state use of the internet as a weapon. The relative unprecedented nature of cyber warfare and the subsequent lack of international customs or practices on the subject have allowed states to "fill the void with their views on how international law applies in this area."[8] Some individual states and organizations have attempted to address this void by creating understandings and guidelines, such as NATO's creation of the Tallinn Manual; however, this manual was never officially adopted and remains more of an idea rather than a practice or custom.[9] Furthermore, many states believe that existing international law can be applied to cyberspace, thereby hindering the creation of new international law on cyberspace.[10] This void in international customs and practices has allowed states such as Russia and the United States to conduct cyber operations, which threaten global and regional stability, without defined consequences. While cyber-attacks certainly violate aspects of Resolution 2625, due to the physical nature of the definition of aggression and the lack of explicit cyber language in Resolution 3314, these attacks fall into a legal grey area in which they are not labelled acts of aggression. The obstacles facing the international community with regard to computer oriented international customs and practices are time, and the ability to create a functional and inclusive definition of cyber warfare.

Defining "Cyber warfare"

As a relatively new development on the international stage, cyber warfare lacks a clear and concise definition. Various countries and even organizations within countries define cyber warfare differently. For example, the U.S. National Research Council's Committee on Offensive Information Warfare does not include cyber-attacks with the goal of information-gathering as meeting the definition of cyber warfare or an offensive cyber-attack, but other organizations such as the U.S. Department of Defense, according to the "DoD Cyber Strategy" drafted in 2015 and still in effect today, consider information-gathering cyber-attacks as a direct threat to national security.[11] Furthermore, other attempts to define and outline responses to cyber-attacks on the international level, such as the Tallinn Manual, fall short as comprehensive approaches to the problem. The Tallinn Manual, created in response to Russian cyber-attacks on Estonia in 2007, is only an understanding among NATO states, not an international legal understanding or agreement. Having individual states or groups such as NATO create their own definitions for an international event such as a cyber-attack further complicates the issue and makes the development of a comprehensive international agreement on cyber warfare more important in order to avoid future conflict. Moreover, as technology advances, cyber weapons can take more varied forms, further hindering any attempts to provide clear or concise definitions. This inability and incoherence in providing a definition of what exactly constitutes an act of cyber warfare invites states to use cyber weapons against each other without conducting an explicit act of aggression.

---

[8] Brian Egan J.D., International Law and Stability in Cyberspace," *Berkeley Journal of International Law.* Nov. 10, 2016. p. 171.

[9] Ibid.

[10] Ibid. 172.

[11] Jordan Peagler, "The Stuxnet Attack: A New Form of Warfare and The (In)Applicability of Current International Law", *Arizona Journal of International and Comparative Law*.; U.S. Department of Defense, "The DoD Cyber Strategy". 2015. p. 10, 13. Accessed 3/4/18. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Furthermore, there remains a question of where cyber warfare and information warfare should be differentiated. Information warfare has multi-faceted definitions for both wartime and peacetime political and social influencing activities. In wartime, "information-based warfare is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage."[12] However, information warfare is also used in non-military applications to influence, manipulate, and control social movements and political discourse.[13] In recent years this non-military application of information warfare has become a pervasive peace-time activity between states. Recent cases, such as Russia's attempts at influencing the U.S. election or Vietnam's attempts to harm U.S.-Philippine relations, prove that cyber warfare contains vast potential for propaganda and information warfare.[14] Should information warfare involving a cyber aspect such as the hacking of emails or recordings of phone calls be considered an act of aggression?

As a concept of international law, the definition of aggression has been critical to the "strengthening of international peace and security," without which it is safe to assume that the world would be in a much more precarious position.[15] Defining aggression through the international legal system and providing a legal framework for responses to aggression have allowed nations to act with surety if they feel they have been attacked by another state. Furthermore, this resolution and framework provides stability to the global environment by allowing all states subject to the international legal system to have a mutual understanding, which works to limit the escalation of conflicts. However, UN General Assembly Resolution 3314, which defines aggression, deals primarily with physical acts of states rather than individuals.[16] Therefore, while aggression and its internationally accepted definition have been highly significant to global stability, the current definition does not adequately cover cyber warfare. However, cyber-attacks, such as the cases discussed below, do violate other international laws such as Resolution 2625, making responding to cyber-attacks complicated.

Many argue that while cyber warfare does break international law, it does not rise to the level of armed force, nor does it meet the current definition of aggression under Resolution 3314.[17] The Russian cyber-attacks on the 2016 U.S. elections and 2008 attacks on Estonia are evidence enough to show that the current legal definition of aggression is inadequate with respect to cyber warfare. These attacks can be directly connected to Russian individuals and, in the case

---

[12] Richard Aldrich, "The International Legal Implications of Information Warfare", *Airpower Journal* Vol. 10, Issue 3 (Fall 1996).

[13] Stephan Blank, "Russian Information Warfare as Domestic Counterinsurgency", *American Foreign Policy Interests* Vol. 35, Issue 1. (2013) p. 32.

[14] David E. Sanger, "Trump's National Security Chief Calls Russian Interference 'Incontrovertible'", *The New York Times*. Accessed 2/17/2018. https://www.nytimes.com/2018/02/17/world/europe/russia-meddling-mcmaster.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection ; Jensen, Valeriano and Maness. "Cyberwarfare", *The Washington Post*. https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/?utm_term=.d4df2c43cb1a

[15] United Nations General Assembly, General Assembly Resolution 3314 Article 3: Definition of Aggression. United Nations, 14 December 1974.Accessed 3/4/18. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement

[16] Elizabeth Wilmshurst. *Definition of Aggression, General Assembly resolution 3314*. United Nations , 14 December 1974.Accessed 3/4/18. http://legal.un.org/avl/ha/da/da.html

[17] Cammack, "The Stuxnet Worm", p. 322.

of Estonia, Russian government addresses can be connected to the assaults.[18] However, due to the nature of cyber warfare, attacks are difficult to attribute directly to state operations. This inability to directly attribute attacks effectively circumvents the international legal system, making individual states solely responsible for their responses to such attacks with limited international legal support. However, U.N. Resolution 2625 states, "Every State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State…when the acts referred to in the present paragraph in a threat or use of force."[19] The word "instigating" indicates that if a state encouraged private individuals, whether through physical or rhetorical support, to conduct cyber-attacks on another state, the sponsoring state would be guilty of a violation of international law. However, this supposes that acts of cyber warfare are indeed acts of aggression and cyber-attacks constitute a use of force, which is not the case in actual practice due to the physical nature of Resolution 3314 and the lack of a cyber warfare component.

U.N. Resolution 3314 Article 3: the Definition of Aggression, lists seven general scenarios, which the international system would consider acts of aggression, such as the crossing of territorial borders with an armed force, the bombardment of a state's territory, or the blockade of a state's ports.[20] In addition, Article 3 states that the list is not exhaustive and the Security Council can include other acts under the definition of an act of aggression.[21] However, while the list presented in Article 3 is not exhaustive, it has "led to a conclusion that only a physical action by a State would be considered an act of aggression."[22] Case studies examined below on cyber-attacks on Estonia, Georgia, Iran, and the United States show that currently, while acts of cyber warfare do violate Resolution 2625, they do not meet the standards of aggression established in the Definition of Aggression, Resolution 3314. These cases highlight the need for the U.N. to incorporate a cyber warfare component to the definition of aggression to avoid future misunderstandings and conflict.

Given the clearly complicated nature of the topic, providing an inclusive and clear definition of cyber warfare is difficult, however, it must be addressed. Cyberwarfare and acts of cyber aggression should be defined in the following manner. Cyber aggression consists of the utilization of computer or internet technology to disrupt or harm a state's ability to function through economic, infrastructural, or political means, including invasive information warfare if it can be directly attributed to state actors. Furthermore, if it is proven that an act came from private individuals of a state, that state is responsible for the apprehension and prosecution of such individuals. If a state does not assist with the apprehension and conviction of an individual who has been proven to be involved in a cyber-attack, that state will be considered to be aiding or otherwise encouraging such an attack, and therefore would be subject to lawful reprisals including, but not limited to, economic sanctions and monetary compensation to the victim state subject to proceedings in the International Court of Justice. While this definition is far from

---

[18] William C. Ashmore, "Impact of Alleged Russian Cyber-attacks," *Baltic Security and Defense Review* Vol. 11, 2009. p. 8.

[19] "U.N. General Assembly Res. 2625 (XXV) (1970)" in *International Law and the Use of Force: Documentary Supplement.* ed. Mary Ellen O'Connell, (New York: Foundation Press, 2005) p. 570-571.

[20] United Nations General Assembly, General Assembly Resolution 3314 Article 3: Definition of Aggression. United Nations, Dec. 14, 1974. Accessed 3/4/18. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement

[21] Ibid.

[22] Cammack, "The Stuxnet Worm", p. 306.

comprehensive, it is written in order to expand progressively with advancements in computer and internet technology as well as address the current issue relating to direct connections to State actors.

Some scholars, such as Nils Melzer, contend that the current international law system can be applied to cyber warfare. Melzer argues that cyber warfare is considered an act of aggression under the U.N. Charter.[23] Furthermore, Melzer contends that logically "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…"[24] In each case study discussed below, cyber warfare was conducted against other states. Yet even in the case of Georgia, where the cyber-attack began weeks prior to the use of conventional forces, the cyber-attack was not taken into consideration when investigating possible acts of aggression.[25]

In spirit, Melzer is correct, the U.N. cannot allow one of the core tenets of its Charter to be so easily circumvented. However, Melzer fails to consider that this circumvention is already occurring in practice due to the lack of a cyber component in Resolution 3314. International laws are created through the formulation of precedents and norms; the longer that cyber warfare remains unaddressed by the U.N. and the international legal system directly, a precedent is being set that cyber warfare can indeed circumvent Resolution 3314. However, Melzer does not entirely neglect the issues facing the international legal system with respect to cyber warfare. He agrees that there remains no consensus on the threshold beyond which a cyber operation amounts to a use of force.[26] This is a crucial problem facing the international community which, without clarification, invites states to conduct increasingly damaging cyber-attacks.

The case studies discussed below will show that while cyber-attacks do violate international law under the 'Friendly Relations' Resolution, the lack of a cyber component in Resolution 3314 as well as the physical nature of the Resolution have allowed states to conduct these attacks without fear of their actions being labelled as aggression. Melzer makes a convincing theoretical argument, but in actual practice, due to the lack of a cyber component in Resolution 3314, cyber warfare has proven in many cases to avoid international legal consequences. This should spur scholars such as Melzer to address the evident gaps in the definition of aggression and strengthen the international legal system involved with cyber aggression.

Estonia

In 2007 and 2008, the countries of Estonia and Georgia suffered large scale cyber-attacks that crippled broad sections of their governments and economies. For nearly a month after announcing a decision to remove a WWII-era Soviet monument, Estonia faced an unrelenting "denial-of-service" (DDOS) cyber-attack on banks, government bodies, media outlets, and telecommunications services in what is known as the Bronze Soldier Incident. This type of cyber-attack overloads networks with requests until the network crashes, effectively 'denying' access to that network or service until the attack stops. Despite Estonia tracing some of the

[23] Nils Melzer, "Cyber Warfare and International Law," p. 7.
[24] Ibid., p. 8.
[25] U.N. Press Release, Security Council Meeting 9419. United Nations. 10 August 2008.
[26] Ibid. p. 9.

DDOS attack to an address associated with the Russian government, Russia denied any official responsibility for the attack on Estonia, suggesting that the attack came from private, pro-Russian activists.[27] Despite economic and governmental damage, Estonia and NATO had few options for retaliation at the time.[28] This type of cyber warfare has been commonly used by state actors in recent years because it does not currently meet the threshold for a military response.[29]

Under Resolution 2625: Friendly Relations

In this case, a foreign state either conducted or encouraged an assault on Estonian infrastructure critical to government and civil function. Estonians used the internet for voting, education, government-civilian dialogue, security, and banking. At the time of the attack, an estimated 95% of banking operations in Estonia were conducted online.[30] The DDOS attack shut down these services and hindered intra-government communication. The damage done by this attack should not be measured in dollars and cents, rather it must be recognized as a violation of the political independence of a State. Estonia had built its government to function as a "paperless government" with the majority of civilian-government interaction occurring online. This attack limited and, in some respects, halted the ability for the Estonian government to communicate with its people. Therefore, this is a violation of Estonian political independence, as Resolution 2625 states, "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference…are in violation of international law."[31] The 'Friendly Relations' Resolution goes on to emphasize that all states have a duty to refrain from "organizing, instigating, assisting or participating in acts of civil strife."[32] In the Bronze Soldier Incident and the resulting cyber-attacks Russia both directly and indirectly involved itself in the internal affairs of another state.[33] Furthermore, NATO and Estonia successfully traced some of the DDOS attacks to Russian government buildings; however, Russia denied involvement in the attack, and rejected to aid in the investigation to find the attackers.[34] First, by denying involvement, Russia is acknowledging that a state's involvement in such an attack is unacceptable under international convention. However, despite this denial, by allowing their territory to be used by non-state actors to launch an attack on another state, Russia is already in violation of international law under Resolution 2625.[35]

---

[27] Matthew Crandall, "Soft Security Threat and Small States: The Case of Estonia," *Defense Studies* Vol. 14, No. 1, 2014. p. 36.

[28] Troy Anderson, "Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals", *Arizona Journal of International and Comparative Law*. 2017.

[29] Damien McGuinness, "How a cyber-attack transformed Estonia", *BBC News*. April 27, 2017. http://www.bbc.com/news/39655415 Accessed: 2/16/2018.

[30] Ashmore, "Impact of Alleged Russian Cyber-attacks," p. 4.

[31] Mary Ellen O'Connell, *International Law and the Use of Force,* p. 570-572.

[32] Ibid., 570-572

[33] Binoy Kampmark, "Cyber Warfare Between Estonia and Russia," *Contemporary Review* Vol. 289, 2007. p. 288-290.

[34] Crandall, "Soft Security Threat," p. 36.

[35] Mary Ellen O'Connell, *International Law and the Use of Force*, p. 570-571.

Under Resolution 3314: Aggression

However, despite the implications of such an attack, and the clear violation of Resolution 2625, this attack does not meet the current definition of aggression under Resolution 3314 Article 3; there was no armed invasion, no border crossed, no bombardment, and no physical damage to the infrastructure. The Definition of Aggression lists physical actions by states, making cyber-attacks, such as the one conducted against Estonia, difficult to concretely label as aggression under the current definition. The lack of a cyber component in the definition of aggression in Resolution 3314 creates a gray area in which cyber warfare is currently stuck in limbo, where it can be both understood as aggression and not aggression. The attack on Estonia resulted in no physical damage, allowing an argument to be made that it was not an act of aggression, despite the attack clearly being intended to inflict harm on another state.[36] Furthermore, scholars such as Larry May consider the "kind of disruption of services that cyber-attacks can achieve is insufficient…" to be considered an act of aggression.[37] The disruptions caused by the cyber-attacks on Estonia did not directly take any lives; therefore, scholars such as May believe that cyber-attacks should not be subject to the laws of war. This divide between cyber-attacks and acts of aggression or war displays the instability that arises in the absence of a cyber component in Resolution 3314. Moreover, it evinces the problem with forcing reality to fit existing laws instead of making laws fit that reality.

Response

In response to this attack, Estonia launched an investigation to positively identify the attackers. However, the Estonian investigators were denied access and aid by the Russian government, limiting the effectiveness of the investigation.[38] Having limited ability to conduct proactive investigations, Estonia and NATO instead invested heavily in cyber security infrastructure and aid. NATO's Computer Emergency Response Teams (CERTs) and the EU's European Network and Information Security Agency both aided in Estonia's recovery and electronic fortification.[39] Furthermore, NATO established its cyber security headquarters, the Cooperative Defense Centre of Excellence in Tallinn, Estonia. Finally, NATO unofficially drafted the Tallinn Manual to better understand cyber warfare; however, NATO does not consider cyber-attacks to be acts of war, and therefore, its member states are not obligated to respond militarily to such an attack.[40] This, in combination with the lack of a cyber component to Resolution 3314 left Estonia, a country with limited means to respond individually against Russia, with no avenues for legal recourse for this attack on their state.

[36] Crandall, "Soft Security Threat," p. 36.

[37] Larry May, "The Nature of War and the Idea of "Cyberwar"", in *Cyberwar: Law and Ethics for Virtual Conflicts* ed. Jens Ohlin, Claire Finkelstein, Kevin Govern (Oxford: Oxford University Press, 2015). p. 9.

[38] Crandall, "Soft Security Threat," p. 36.

[39] Stephen Herzog, "Revisiting the Estonian Cyber-attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* Vol. 4, No. 2, Summer 2011. p 53-54.

[40] Crandall, "Soft Security Threat," p. 36.

Georgia

The cyber-attack on Georgia represents a similar style of attack as was conducted against Estonia. In this case, Russia used a denial of service attack against the Georgian government in the days prior to the commencement of the conventional conflict on August 8, 2008. The cyber-attack intensified once open hostilities began between Russia and Georgia, with a denial of service attack targeting government servers, media outlets, and telecommunication services. This cyber-attack successfully and effectively limited the Georgian government's ability to communicate with its citizens as well as sympathizers around the world. The cyber-attack contained two stages: first, in the days leading up to the conventional invasion by Russian forces, Georgian electronic infrastructure suffered massive DDOS attacks, effectively isolating the nation from global communication.[41] While first stage continued, the second stage coincided with the launching of the Russian conventional invasion and targeted economic infrastructure such as banks and media outlets, which limited the ability of the Georgian government to disseminate information to their citizens, and inflicted significant harm to the national economy.[42]

While Russia has denied responsibility for the cyber-attacks in Georgia, and there is no conclusive evidence of their involvement, many national security and cyber warfare experts believe it was a Russian government operation.[43] While he did not directly connect Russia to the cyber-attacks, Colonel Anatoly Tsyganok, the head of the Russian Military Forecasting Center stated that the Russian cyber campaign focused on information warfare against the Georgian government. The goal of this campaign was to "isolate and silence" the Georgian government and media.[44]

Under Resolution 2625: Friendly Relations

This attack occurred in the lead up to and during the conventional military conflict between Russia and Georgia in 2008. Examining the cyber aspect of this conflict separately from the conventional conflict makes clear that Russia violated international law under Resolution 2625. Similar to the attack on Estonia, this attack came from Russian territory. Furthermore, the Russian government denied involvement and refused to aid in any investigation.[45] With regard to Georgia, at best, Russia allowed their territory to once again be used in an assault on another state. At worst, as the analysis from leading cyber security experts would suggest, the Russian government facilitated and aided non-state actors in the assault on Georgia.[46] In either case, Russia violated the 'Friendly Relations' Resolution by allowing their territory to be used by non-state actors to launch an attack on another state.

---

[41] Cpt. Paulo Shakarian, PH.D., "The 2008 Russian Cyber Campaign Against Georgia" *Military Review* Nov.-Dec. 2011. p. 63-64.

[42] Ibid. p. 65-66.

[43] John Markoff, "Before the Gunfire, Cyberattacks", *The New York Times*. August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html Accessed 2/16/2018.

[44] Cpt. Paulo Shakarian, "The 2008 Russian Cyber Campaign," p. 65-66.

[45] Andrzej Kozlowski, "Comparative Analysis of Cyber-attacks on Estonia, Georgia, and Kyrgyzstan," *European Scientific Journal* Vol. 3 February 2014. p. 240.

[46] Cpt. Paulo Shakarian, "The 2008 Russian Cyber Campaign," p. 64-65, 67.; Andrzej Kozlowski, "Comparative Analysis of Cyber-attacks," p. 240.

Under Resolution 3314: Aggression

As in the case of Estonia, the cyber-attacks in Georgia do not clearly meet the U.N. definition of an act of aggression due to the lack of a cyber component to the Definition of Aggression and the physical nature of the language used in the Resolution. Both the Georgian and Russian conventional military actions that followed could be considered acts of aggression, but the cyber aspect of the conflict was largely ignored, and attempts by the U.N. Security Council to attribute aggression focused solely on the conventional actions of Russia and Georgia.[47] The failure of the U.N. Security Council to consider the cyber-attacks when investigating aggression in this conflict establishes the notion that under the current definition, cyber-attacks are not interpreted as aggression. Indeed, had this attack taken place without a corresponding conventional conflict, the events would not have met the definition for an act of aggression. While this cyber-attack limited the flow of information within Georgia, it did not harm any physical infrastructure, and did not meet any of the seven general scenarios listed by UN Resolution 3314, Article 3. Furthermore, Resolution 3314 focuses entirely on physical actions of states or state-actors. In this cyber-attack, Russia either directly or indirectly supported non-state actors in a non-physical assault, which certainly violates Resolution 2625, but is not currently understood to meet the definition of aggression under Resolution 3314. Moreover, similar to the attack on Estonia, some believe that cyber-attacks that disrupt services and communication do not rise to the level of aggression.[48] If the international legal definition of an act of aggression had incorporated a cyber aspect, such as the definition proposed in this article, Russia may have been declared the aggressor, since the cyber-attack began weeks prior to the conventional conflict. Thus, the Georgian case is a clear example of the lack of an inclusive cyber warfare definition in Resolution 3314 leading to a failure of that system in maintaining peace and stability around the world.

Response

Numerous outside technologies and cyber-security organizations, both private and governmental, assisted Georgia in its recovery from this attack. Estonia, having recently been the subject of similar attacks, sent two CERTs experts to help establish better network security. Furthermore, other states, such as Poland, attempted to aid Georgian communication by posting messages on their websites from the Georgian government to the Georgian people during the attacks. [49] As an official response, Georgia attempted to use established U.N. channels to blame Russia for an act of aggression; however, as discussed above, the cyber-attacks were not considered when determining which state was the aggressor. These limitations restricted Georgia's ability to seek redress or respond in kind.

The attacks in Estonia and Georgia represent examples of one of the most straight forward cyber-attack methods. Additionally, these attacks show how difficult it is to find conclusive evidence of a foreign government's involvement. In both cases, both Georgia and Estonia had limited legally recognized response or retaliation options. Not only were they limited by their own capabilities, the absence of an explicit cyber component in Resolution 3314 also

[47] UN Press Release, Security Council Meeting 9419. United Nations. 10 August 2008.

[48] Larry May, "The Nature of War," p. 9.

[49] Ashmore, "Impact of Alleged Russian Cyber-attacks," p. 11.

limited their avenues for retaliation or compensation. Due to the complicated nature and fast advancement of cyber warfare, antiquated international legal systems held no protections or avenues of redress for a victim state. The Tallinn Manual attempted to remedy this; however, as discussed above, even this document falls short of articulating allowable protective measures or systems of retaliation. Furthermore, the Tallinn's Manual is only unofficially used by NATO members and not recognized at all by the international legal system.[50]

U.S. Stuxnet Attack on Iran

One of the most well-known cases of international cyber-attacks is the Stuxnet and Flame attacks on the Iranian nuclear program initiated by the United States and Israel. Discovered in 2010, the Stuxnet malware targeted Iran's centrifuges and, through malicious coding, caused the centrifuges to destroy themselves. Designed to be a persistent attack, Stuxnet's coding hid the malware from Iranian engineers, allowing it to damage or destroy approximately 1,000 of Iran's centrifuges, setting the Iranian nuclear program back an estimated two years.[51] Opposing Iran's nuclear advancements, the United States and Israel sought to slow progress while a solution could be found.[52]

This attack represented a new and more aggressive form of cyber weaponry. Prior to Stuxnet, cyber warfare remained largely within the scope of information gathering or "denial-of-service" attacks, with only a few small-scale instances of cyber weapons being used to cause physical infrastructural damage. To many cyber experts, this incident was a turning point in the realm of cyber warfare. This case provided evidence that cyber weapons can act in a similar fashion to conventional weapons in their ability to destroy or dismantle infrastructure.[53]

Under Resolution 2625: Friendly Relations

The 'Friendly Relations' Resolution 2625 states, "States parties to an international dispute, as well as other States, shall refrain from any action which may aggravate the situation so as to endanger the maintenance of international peace and security."[54] Furthermore, Resolution 2625 specifies that states cannot use force or coercion to subvert another state's sovereign rights.[55] Sovereignty is the principle that states have supreme authority within their own borders, and can only be limited by external laws if they consent.[56] By using Stuxnet, the U.S. government sought to hinder the Iranian nuclear program, a program which the Iranian government desired. This is a clear violation of Iranian sovereignty, and therefore a violation of Resolution 2625.

---

[50] Egan, "Stability in Cyberspace," p. 171.

[51] Ralph Langer, "Stuxnet's Secret Twin", *Foreign Policy*. November 19, 2013. http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/ Accessed 2/16/2018.

[52] Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say", *The Washington Post*. June 2, 2012. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.075bbf250423 Accessed: 2/16/2018.

[53] Ibid.

[54] Mary Ellen O'Connell, *International Law and the Use of Force*, p. 570-572.

[55] Ibid.

[56] David Bederman, *International Law Frameworks* (New York: Foundation Press, 2001) p. 50.

Under Resolution 3314: Aggression

Given the destruction of one state's physical infrastructure by a foreign state, the Stuxnet attack should be considered an act of aggression under Article 2 of the United Nations Charter.[57] Furthermore, this U.S./Israeli action directly led to the physical destruction of Iranian infrastructure which, under the current interpretation of Resolution 3314 Article 3, would constitute an act of aggression.[58] However, the fact that the initial action occurred in cyberspace confuses the subject, and by a rigid interpretation of Article 3, might not be classified as an act of aggression. Under the Definition of Aggression, the physical crossing of borders by physical bodies, be they human or armament, is an act of aggression. However, arguments can and have been made that a cyber-attack does not represent a physical event, and therefore, does not constitute an act of aggression or war.[59] This case study shows that without a focused cyber warfare addition to Resolution 3314 Article 3, an attack as straightforward as the Stuxnet virus can circumvent Resolution 3314. This places the world in a more precarious position, where states may assault each other using cyber weapons without worrying about the victim state being able to invoke Article 2. The addition of explicit cyber language to the Definition of Aggression would resolve any issues involving the interpretation or misinterpretation of the language in Resolution 3314 and make clear that cyber-attacks are indeed acts of aggression.

Response

The Iranian government, similar to the previous victim states discussed, found itself in an untenable position when attempting to respond to this attack. First, as with the attacks on Estonia and Georgia, cyber weapons remain extremely difficult to trace to their origination point. While circumstantial evidence points to the U.S. and Israeli governments, at the time, there was no conclusive evidence that Iran could use to officially accuse the two nations.[60] Secondly, similar to the attacks in Estonia and Georgia, no agreed upon system for responding to cyber warfare existed at the time.[61] Due to the lack of such a system, if Iran responded with a conventional attack on Israel, they would have risked being labeled the aggressor in the eyes of the international system, despite simply responding to a damaging attack on their state infrastructure. Instead, Iran strengthened its own electronic fortifications, and is suspected of having launched a series of increasingly sophisticated attacks in retaliation against both the United States as well as other states is the region.[62] If the Definition of Aggression Resolution included a cyber warfare component, such as that proposed in this article, Iran would have been on stable legal ground to accuse the U.S. of an act of aggression. The inclusion of this cyber component would have allowed for a more stable response, from both Iran and the international community, to the attack.

---

[57] Matthew Hoisington, "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense" *Boston College International and Comparative Law Review*, 2009/04/01, Vol: 32, p 446-447.

[58] Cammack, "The Stuxnet Worm," p. 306.

[59] Larry May, "The Nature of War," p. 8.

[60] Cammack, "The Stuxnet Worm," p. 318.

[61] Anderson, "Fitting a Virtual Peg into a Round Hole."

[62] Andrea Shalal-Esa, "Iran Strengthen Cyber capabilities after Stuxnet," *Reuters.* January 17, 2013. https://www.reuters.com/article/us-iran-usa-cyber/iran-strengthened-cyber-capabilities-after-stuxnet-u-s-general-idUSBRE90G1C420130118 Accessed: 4//4/2018.

The Philippines

The latest and currently most popular use of cyber weapons is to use these tools to wage information warfare. For example, in 2017, it is suspected but not conclusively proven that Vietnam or a group closely associated with the Vietnamese government launched a cyber espionage attack, which resulted in the release of private communications between United States President Trump and Philippine President Duterte.[63] Vietnam sought to expose warming relations between the Philippines and China, potentially harming U.S.-Philippines relations.[64] This attack and the subsequent release of private communications represent the latest evolution in the use of cyber weapons on the international political stage. Such attacks do not aim to physically damage infrastructure, an economy, or communications systems, but rather to publicize politically damaging information.

This case study presents an important issue in the debate over cyber warfare: when does information warfare in the digital age transition into an act of aggression? The hacking group, OceanLotus, a group indirectly connected to the Vietnamese government, used cyber-attacks against Philippine state agencies to attain sensitive data, and subsequently used the release of that data to damage the relations between the Philippines and China.[65] Such a release of information does not and should not be considered an act of aggression. However, the cyber aspect of this attack should be considered as a potential violation of Article 2, as the cyber-attack and the resulting release of sensitive data posed the risk of destabilizing diplomatic relations in the region.[66]

Under Resolution 2625: Friendly Relations

If evidence can be found directly linking the Vietnamese government to this attack, it most certainly is a violation of international law under Resolution 2625. As discussed in the previous case studies, the 'Friendly Relations' Resolution states that no state may interfere with the sovereign rights or political independence of another. The goal of this attack was to influence the Philippine-U.S. relationship; therefore, it was an attack on Philippines' sovereignty and political independence.[67] Furthermore, Resolution 2625 makes clear that even though Vietnam is only indirectly linked to the OceanLotus group, their actions may still violate international law by allowing the attack to be executed from within their territory.

---

[63] Adam Segal, "Frustrated with the Philippines, Vietnam Resorts to Cyber Espionage", *Council on Foreign Relations*. June 8, 2017. https://www.cfr.org/blog/frustrated-philippines-vietnam-resorts-cyber-espionage Accessed: 2/16/2018.

[64] Ibid.

[65] Reuters Staff, "Vietnam-linked hackers likely targeting Philippines over South China Sea dispute: FireEye," *Reuters*. May 25, 2017. Accessed: 3/25/18. https://www.reuters.com/article/us-cyber-philippines-southchinasea/vietnam-linked-hackers-likely-targeting-philippines-over-south-china-sea-dispute-fireeye-idUSKBN18L1MR

[66] Segal, "Frustrated with the Philippines," https://www.cfr.org/blog/frustrated-philippines-vietnam-resorts-cyber-espionage

[67] Ibid.

Under Resolution 3314: Aggression

As Resolution 3314 is currently written, this cyber-attack and the resulting release of information is not a violation. There is not a physical aspect to this attack which could meet any of the examples of aggression in the current definition. Furthermore, unlike the previous case studies of Estonia and Georgia, this attack did not hinder the economy, media, or telecommunications. While Resolution 3314 protects political independence, the nature of its language has led to a belief that only *physical* actions by states may violate the resolution.[68] Therefore, despite the harm to Philippines' political independence and sovereignty and the stability of the region, this attack does not violate Resolution 3314 under its current interpretation. Additionally, the lack of a clear cyber component to the definition of aggression leaves a void in which this attack might be understood to not be an act of aggression.

Response

Both the Philippines and the United States were limited in their response options to this attack. First, the information warfare side of this attack is not and should not be considered an act of aggression. Furthermore, due to the limitations of the current definition of aggression under Resolution 3314, neither victim state could respond with force under international law. In this case, there seems to have been almost no response from either the Philippines or the United States.

Russia 2016 U.S. Election

An additional example of the use of cyber weapons in information warfare is Russian attempts to influence the 2016 U.S. elections and exacerbate divisions among U.S. citizens. It is alleged that Russian state actors conducted cyber-attacks to access email servers owned by the Democratic National Committee (DNC) and subsequently released damaging information in an attempt to disrupt the U.S. democratic process.[69] Complicating this attack, it is also alleged that numerous private Russian citizens conducted a coordinated campaign which included identity theft and extensive use of social media platforms to sow divisions and exacerbate tensions between U.S. citizens on flash point issues such as immigration.[70] The U.S. Director of National Intelligence (DNI) released a report titled, "Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution," which makes clear the U.S. intelligence communities' opinion that the Russian government directly conducted cyber campaigns to influence the 2016 U.S. presidential election.[71] These attacks on the U.S. democratic system are just that, attacks, by one state on another.

---

[68] Cammack, "The Stuxnet Worm," p. 306.

[69] Jonathan Masters, "Russia, Trump, and the 2016 U.S. Election" *Council on Foreign Relations*. February 26, 2018. Accessed: 3/4/18. https://www.cfr.org/search?keyword=Russia+U.S.+election

[70] Matt Apuzzo, "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign," *The New York Times*. February 16, 2018. Accessed: 3/4/18. https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html

[71] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution", United States National Intelligence Council, January 6, 2017. p. 1-2. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Under Resolution 2625: Friendly Relations

If the evidence discussed in the DNI report is taken as fact, this attack is undoubtedly a violation of international law under Resolution 2625. The government of Russia used a cyber campaign, which included the theft of communications and subsequent release of those communications to directly influence the political process of the United States. This is a clear violation of Resolution 2625. Furthermore, this campaign aimed to disrupt national unity and harmed U.S. political independence, both of which are violations of Resolution 2625, which states that, "…any attempt aimed at the partial or total disruption of national unity…or at its political independence is incompatible with the purposes and principles of the Charter."[72] These actions are certainly not the actions of a friendly nation and are clearly violating Resolution 2625; however, they do not rise to the level of aggression under the current definition.

Under Resolution 3314: Aggression

Current international law might hold that it was potentially a state attack on a private company, the DNC, with no economic or infrastructural damage, therefore not meeting the definition of an act of aggression. Alternatively, it could be argued that it was private Russian citizens conducting this information warfare, thus placing the case outside the jurisdiction of the international legal system. Additionally, while these cyber-attacks were meant to influence the political independence of a state, they do not clearly meet the threshold of 'an act of aggression' under Resolution 3314 Article 3, because no physical armed force was used. Moreover, the lack of an explicit cyber component in the definition of aggression creates a grey area in which attacks such as this are not labelled as aggression. This attack represents a failure of the international legal system to maintain and protect stability. Furthermore, because these attacks do not meet the international legal definition of aggression, the U.S. has limited options to respond that are justifiable under international law.

Response

In response to these attacks, the United States placed sanctions on Russian individuals and companies and government entities. These sanctions largely targeted individuals and private entities rather than the Russian government itself due to the difficulty in attributing the attacks. However, two government organizations were sanctioned in this action, the Russian Federal Security Service, and the GRU, Russia's chief military intelligence agency. [73] When compared to the responses in the other case studies, this response may seem more complete and proactive. However, it remains concerning that a cyber-attack of this magnitude, with direct attribution to a foreign government, only warranted limited sanctions. This response indicates that cyber-attacks continue to be understood as unfriendly acts of states, rather than as acts of aggression under Resolution 3314.

[72] Mary Ellen O'Connell, *International Law and the Use of Force*, p. 569, 572.

[73] Ryan Lucas, Tamara Keith. "U.S. Imposes New Sanctions On Russia Over Election Interference, Cyberattacks," *National Public Radio* March 15, 2018. https://www.npr.org/2018/03/15/593895383/us-imposes-new-sanctions-on-russia-over-election-interference-cyberattacks

States' Right to Respond

Given these examples of the evolution of cyber weapons as both tools of war as well as political coercion, and the failure of Definition of Aggression Resolution to adequately address this new weapon, it is clear that these attacks will continue to occur. However, until Resolution 3314 is amended to include cyber-attacks, states maintain the right to respond to such attacks with any means at their disposal. Sovereign states have a natural right to respond forcefully if they feel they have been attacked. Sovereignty in international law is an essential principle, both to domestic and international order.[74] Anél Ferreira-Snyman notes that state sovereignty, which is generally accepted as a fundamental principle of international law, upholds three norms: "first, that all sovereign States, irrespective of their size, have equal rights. Second, that the territorial integrity and political independence of all sovereign States is inviolable. Third, that intervention in the domestic affairs of sovereign States in not permissible."[75] Furthermore, according to David Bederman, principle of sovereignty holds "that each nation answers only to its own domestic order and is not accountable to a larger international community, save only to the extent it has consented to do so."[76] Using the principle of sovereignty, a state may take retaliatory action when threatened or harmed by another state, without consent or agreement from the international community. This concept is in fact enshrined in Article 51 of the U.N. Charter, which explicitly recognizes the "inherent right of individual or collective self-defense."[77] Moreover, J.L. Brierly contends that if international law fails to protect a victim state, or give that victim state a legal avenue for redress, "it is likely that the injured state, if it is strong enough, will seek by other means the redress that the law cannot afford it."[78] In the case studies examined above, all of the victim states could have responded with cyber-attacks of their own or conventional means as deemed necessary. Until the international legal system develops adequate definitions and frameworks for dealing with this new arena of conflict, states can defend themselves and retaliate as they see fit. Therefore, not having a cyber element to the U.N. definition of aggression threatens international stability. It is widely accepted that states may respond to threats or attacks in any manner they choose, including conventional armed attacks, and are only restricted by proportionality and the laws of war.[79] Furthermore, the lack of a cyber component may also limit a state's legal ability to respond to these attacks. States such as Iran were limited in their response due to the ambiguity of Resolution 3314 on cyber-attacks. Due to the risk of being labelled the aggressor if they responded using conventional means, Iran instead chose to conduct cyber-attacks of their own. This response has the potential to create a series of increasingly damaging assaults between two states, which Resolution 3314 is unable to address. This void in legal structure creates instability.

As part of the discussion on states' right to respond to cyber-attacks, there is debate over whether a cyber-attack constitutes a violation of the state's territorial integrity. The idea of defined borders and the defense of territorial integrity is integral to the defense of a state's

---

[74] Brierly, *The Law of Nations*, p. 10.

[75] Anel Ferreira-Snyman, "Sovereignty and the changing nature of Public International Law: Towards World Law?" *The Comparative and International Law Journal of Southern Africa* Vol. 4 No. 3 (November 2007), p. 406-407.

[76] David Bederman, *International Law Frameworks* (New York: Foundation Press, 2001), p. 50.

[77] United Nations Charter: Article 51, United Nations (26 June 1945). http://www.un.org/en/sections/un-charter/chapter-vii/index.html Accessed: 4/18/2018.

[78] Brierly, *The Law of Nations*, p. 75.

[79] Bederman, *International Law Frameworks*, p. 219.

sovereignty.[80] Some scholars contend that cyber-attacks do not meet the threshold to be considered violations of a state's territory, and therefore are not acts of war.[81] However, it must be understood that if a state were to decide that a cyber-attack constitutes a violation of territorial integrity, they could respond with a conventional military attack. Victim states have an "inherent right" to self-defense protected by the U.N. Charter, and in the exercise of that right, states have no legal requirement to seek the approval of the U.N. or any other international body.[82] The state's ability to act unilaterally when responding to threats or aggressions of another state is undeniable. This ability to respond unilaterally and without condition, except proportionality and the laws of war, to cyber-attacks makes the addition of a cyber warfare component to Resolution 3314 imperative.

Furthermore, under the Effects Doctrine, victim states automatically hold jurisdiction over a cyber-attack if that attack inflicted economic costs. The Effects Doctrine "permits the exercise of jurisdiction over the extraterritorial activities of foreigners which produce economic effects within the territory."[83] Under this doctrine, states may hold foreign non-state actors legally responsible for cyber-attacks that caused economic damages. For example, in the Estonia case study, one bank reported $1 million dollars in damages. If the Estonian government could trace the attack to an individual operating in Russia, that individual would be subject to Estonian law for their actions.[84] Through the Effect Doctrine, regardless of whether cyber-attacks are understood as aggression or not, individuals who conduct these attacks are automatically subject to the victim state's judicial system.

Conclusion

The case studies discussed here provide evidence of not only an increase in cyber weapon use, but also the varied formats in which they have been utilized. These variations display why it remains difficult to provide a succinct definition to these new weapons. Yet, without a clear understanding of the danger these new weapons bring, along with the addition of a cyber component to the Definition of Aggression in Resolution 3314, there is the risk that cyber-attacks may act as a catalyst to conventional warfare. Laws must be made to fit reality. Attempting to force reality to fit laws creates gaps in understanding and protection, which endanger global peace and stability. As long as states believe that cyber warfare is not an act of aggression, they will continue to use these weapons, thereby endangering global stability. The case studies above prove that while cyber warfare certainly violates the 'Friendly Relations' Resolution 2625, it does not meet the definition of aggression under Resolution 3314. This gap in international law has created an unstable global environment, in which states are conducting increasingly damaging cyber-attacks against one another, and places victim states on unstable legal ground concerning retaliation. The inclusion of cyber warfare and its definition to Resolution 3314 Article 3 will help prevent the use of these destabilizing weapons in the future. However, until such a framework exists within the international legal system, states should

[80] Bederman, *International Law Frameworks*, p. 51.

[81] Larry May, "The Nature of War,", p. 8.

[82] Karl M. Meessen, "Unilateral Recourse to Military Force Against Terrorist Attacks," in *International Law and the Use of Force*. ed. Mary O'Connell,. p. 584.

[83] Vaughan Lowe, International Law and the Effects Doctrine in the European Court of Justice," *The Cambridge Law Review* Vol. 48, Issue 1 (March, 1989). p. 9.

[84] Herzog, "Revisiting the Estonian Cyber-attacks," p 51-52.

maintain the right to respond to cyber-attacks by any reasonable means at their disposal. These response options should include the use of conventional weapons if the cyber-attack is deemed harmful to state economies, infrastructure, or political institutions. Moreover, a robust and immediate conversation within the international community is imperative to address the lack of understanding of cyber warfare as a weapon of war, to better define what constitutes an act of war in this new cyber dimension, and how states should respond to such attacks. Without this conversation and a cyber warfare addition to Resolution 3314, cyber-attacks will continue to have the potential to escalate into conventional war and the current global instability will continue.

Bibliography

Aldrich, Richard. "The International Legal Implications of Information Warfare." *Airpower Journal* Vol. 10, Issue 3 (Fall 1996).

Anderson, Troy. "Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals." *Arizona Journal of International and Comparative Law* Vol. 35 (2017): 135.

Apuzzo, Matt. "13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign." *The New York Times*. February 16, 2018. https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html

Arend, Anthony. "International Law and the Preemptive use of Military Force." *The Washington Quarterly* Vol. 26, no. 2 (Spring 2003): 89-103.

Ashmore, William C. "Impact of Alleged Russian Cyber-attacks." *Baltic Security and Defense Review* Vol. 11, Issue 1 (2009): 4-40.

Bederman, David. *International Law Frameworks.* New York: Foundation Press, 2001.

Blank, Stephan. "Russian Information Warfare as Domestic Counterinsurgency", *American Foreign Policy Interests* Vol. 35, Issue 1. (2013).

Brierly, J.L. *The Law of Nations: An Introduction to the International Law of Peace.* Oxford: Oxford University Press, 1963.

Cammack, Chance. "The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression." *Tulane Journal of International and Comparative Law*, Vol. 20 (January 1, 2011): 303.

Crandall, Matthew. "Soft Security Threat and Small States: The Case of Estonia." *Defense Studies* Vol. 14, No. 1 (2014): 30-55.

Dev, Priyanka. ""Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," *Texas International Law Journal* Vol. 50, Issue 2 (Spring 2015) 379-399.

Egan, Brian. "International Law and Stability in Cyberspace." *Berkeley Journal of International Law* Vol. 35, Issue 1 (Nov. 10, 2016): 169-180.

Ferreira-Snyman, Anel. "Sovereignty and the changing nature of Public International Law: Towards World Law?" *The Comparative and International Law Journal of Southern Africa* Vol. 4, No. 3 (November 2007) 406-407.

Herzog, Stephen. "Revisiting the Estonian Cyber-attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* Vol. 4, No. 2 (Summer 2011).

Hoisington, Matthew. "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense" *Boston College International and Comparative Law Review* Vol: 32 (April 1, 2009): 439.

International Court of Justice. Statute of the International Court of Justice, Article 38. United Nations.

Jensen, Benjamin, Maness, Ryan C., and Valeriano, Brandon. "Cyberwarfare has taken a new turn. Yes, it's time to worry." *The Washington Post*. July 13, 2017. https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/?utm_term=.41b9f74519ec

Kampmark, Binoy. "Cyber Warfare Between Estonia and Russia." *Contemporary Review* Vol. 289 (2007).

Keith, Tamara, Lucas, Ryan. "U.S. Imposes New Sanctions on Russia Over Election Interference, Cyberattacks," *National Public Radio* March 15, 2018. https://www.npr.org/2018/03/15/593895383/us-imposes-new-sanctions-on-russia-over-election-interference-cyberattacks

Kozlowski, Andrzej. "Comparative Analysis of Cyber-attacks on Estonia, Georgia, and Kyrgyzstan," *European Scientific Journal* Vol. 3 (February 2014).

Langer, Ralph. "Stuxnet's Secret Twin." *Foreign Policy*. November 19, 2013. http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

Lowe, Vaughan. "International Law and the Effects Doctrine in the European Court of Justice," *The Cambridge Law Review* Vol. 48, Issue 1 (March 1989).

Markoff, John. "Before the Gunfire, Cyberattacks." *The New York Times*, August 12, 2008. http://www.nytimes.com/2008/08/13/technology/13cyber.html

Masters, Jonathan. "Russia, Trump, and the 2016 U.S. Election." *Council on Foreign Relations*. February 26, 2018. https://www.cfr.org/search?keyword=Russia+U.S.+election

May, Larry. "The Nature of War and the Idea of "Cyberwar"", in *Cyberwar: Law and Ethics for Virtual Conflicts*. Edited by Jens Ohlin, Claire Finkelstein, Kevin Govern. Oxford: Oxford University Press, 2015.

McGuinness, Damien. "How a cyber-attack transformed Estonia." *BBC News*, April 27, 2017. http://www.bbc.com/news/39655415

Meessen, Karl M. "Unilateral Recourse to Military Force Against Terrorist Attacks," in *International Law and the Use of Force*. Edited by Mary O'Connell. New York: Foundation Press, 2005.

Nakashima, Ellen and Warrick, Joby. "Stuxnet was work of U.S. and Israeli experts, officials say." *The Washington Post*. June 2, 2012. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.075bbf250423

Nils Melzer, "Cyber Warfare and International Law," United Nations Institute for Disarmament Research. 2011.

O'Connell, Mary Ellen, ed. *International Law and the Use of Force: Documentary Supplement.* New York: Foundation Press, 2005.

Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution", United States National Intelligence Council, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Peagler, Jordan. "The Stuxnet Attack: A New Form of Warfare and the (In)Applicability of Current International Law." *Arizona Journal of International and Comparative Law* Vol. 31(July 1, 2014).

Reuters Staff. "Vietnam-linked hackers likely targeting Philippines over South China Sea dispute: FireEye." *Reuters*. May 25, 2017. https://www.reuters.com/article/us-cyber-philippines-southchinasea/vietnam-linked-hackers-likely-targeting-philippines-over-south-china-sea-dispute-fireeye-idUSKBN18L1MR

Sanger, David E. "Trump's National Security Chief Calls Russian Interference 'Incontrovertible'." *The New York Times*, February 17, 2018. https://www.nytimes.com/2018/02/17/world/europe/russia-meddling-mcmaster.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection

Segal, Adam. "Frustrated with the Philippines, Vietnam Resorts to Cyber Espionage." *Council on Foreign Relations*. June 8, 2017. https://www.cfr.org/blog/frustrated-philippines-vietnam-resorts-cyber-espionage

Shakarian, Paulo. "The 2008 Russian Cyber Campaign Against Georgia." *Military Review* Vol. 91, Issue 6 (Nov.-Dec. 2011): 63-68.

Shalal-Esa, Andrea. "Iran Strengthen Cyber capabilities after Stuxnet," *Reuters.* January 17, 2013. https://www.reuters.com/article/us-iran-usa-cyber/iran-strengthened-cyber-capabilities-after-stuxnet-u-s-general-idUSBRE90G1C420130118

United States Department of Defense, *The Department of Defense Cyber Strategy*. United States Government, Department of Defense (2015). Accessed 3/4/18.https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

United Nations General Assembly. Definition of Aggression, General Assembly Resolution 3314, 14 December 1974.Accessed 3/4/18. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement

United Nations. U.N. Press Release, Security Council Meeting 9419, 10 August 2008.

United Nations. United Nations Charter, Article 2(4). United Nations. 26 June 1945. http://www.un.org/en/sections/un-charter/chapter-i/index.html

United Nations. United Nations Charter: Article 51. United Nations. 26 June 1945. http://www.un.org/en/sections/un-charter/chapter-vii/index.html

Wilmshurst, Elizabeth. "Definition of Aggression, General Assembly Resolution 3314." United Nations. Accessed 3/4/18. http://legal.un.org/avl/ha/da/da.html