11-12-2019

How Effective Are Current International Laws in Combating Issues of Global Cyber Security?

Jessica E. Chadwick Cordero
Florida International University, jchad011@fiu.edu

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

HOW EFFECTIVE ARE CURRENT INTERNATIONAL LAWS IN COMBATING ISSUES OF GLOBAL CYBER SECURITY?

A thesis submitted in partial fulfillment of

the requirements for the degree of

MASTER OF ARTS

in

INTERNATIONAL STUDIES

by

Jessica Chadwick Cordero

2019

To: Dean John F. Stack
Steven J. Green School of International and Public Affairs

This thesis, written by Jessica Chadwick Cordero, and entitled How Effective are Current International Laws in Combating Issues of Cyber Security? having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this thesis and recommend that it be approved.

Mohiaddin Mesbahi

Thomas A. Breslin

Harry Gould, Major Professor

Date of Defense: November 15, 2019

The thesis of Jessica Chadwick Cordero is approved.

Dean John F. Stack
Steven J. Green School of International and Public Affairs

Andrés G. Gil
Vice President for Research and Economic Development and Dean of the University Graduate School

Florida International University, 2019

DEDICATION

To my mamá, who always believed in me.

ACKNOWLEDGMENTS

Without the help of several important people in my life, it would be hard to imagine that I would have gotten this far in my career. First of all, I would like to thank my mother. She has supported and encouraged me to keep learning and challenging myself from a very early age, always providing me with new materials and ideas to explore. It is without a doubt, that my mother has been the one who has played the most important role in shaping my determination to constantly be better, and to keep striving to achieve what others told me was simply impossible. Second, I would like to thank my family who has not only supported me throughout my career, but also in contributing to the events that brought me to start my university career in the United States. Third, I would also like to thank Gabriela Ramos, who has been the most important figure in my life with regard to making me believe that I am capable and worthy of my career, and who has helped me every single step of the way. Gabi has supported me on a daily basis without fail, whether good or bad, and it is thanks to her that I will graduate with my head held high. Lastly, I would like to thank my friends in the Department ofPolitics and International Relations who have guided me through graduate school since the very first day, and who also allowed me to believe that I could achieve what I once thought was not attainable for me. A very special thanks to Dr. Gould, Dr. Breslin, and Dr. Mesbahi who inspired not just me, but also the theme of my thesis.

ABSTRACT OF THE THESIS

HOW EFFECTIVE ARE CURRENT INTERNATIONAL LAWS IN COMBATING ISSUES OF GLOBAL CYBER SECURITY?

by

Jessica Chadwick Cordero

Florida International University, 2019

Miami, Florida

Professor Harry Gould, Major Professor

One of the most serious threats or challenges to national and international security that we are facing today is cyber security. Currently, there are no bodies of international law that can be applied in order to hold states accountable for launching cyber-attacks against other states, and thus it is imperative that several obstacles be removed in order for the law to be applicable before we find ourselves in an all-out “World War C” (Segal, 2016). Critical infrastructure systems are at great risk from attacks that could lead to catastrophic events such as total power blackouts, the opening of dams, and serious economic turmoil. There is no doubt that we are on the brink of a very serious threat to international security, and the current inapplicability of international humanitarian law to this new realm of warfare is sincerely alarming.

TABLE OF CONTENTS

CHAPTER PAGE

LIST OF ACRONYMS

APT: Advanced Persistent Threat

CNAP: Cyber National Security Action Plan

DDoS: Distributed Denial of Service

DoD: Department of Defense

DHS: Department of Homeland Security

DoS: Denial of Service

DPH: Direct Participation in Hostilities

DNC: Democratic National Committee

ISIS: Islamic State of Iraq and Syria

IHL: International Humanitarian Law

ILC: International Law Commission

ICJ: International Court of Justice

LOAC: Laws of Armed Conflict

NATO: North Atlantic treaty Organization

NSA: National Security Agency

PLA: People’s Liberation Army

PRC: People’s Republic of China

P2P: Peer to Peer

RAT: Remote Access Trojan

SCADA: Supervisory Control and Data Acquisition

SVR: Russia’s Foreign Intelligence Service

TAO: Tailored Operations Group

CHAPTER ONE

Overview of the Issue

The first problem in applying existing international law is that there is no agreed definition of what cyber-attack, cyber threat, cyber weapon, or cyber warfare mean. The second problem is that though individual states have their own national definitions, there must be a consensus among the international community on those definitions in order for international law to be applicable. The third problem in applying international humanitarian law to cyber hostility is the issue of accountability and anonymity. Cyber-attacks are anonymous by nature, and according to Article 51 of the United Nations Charter, the state must be able to adequately hold a state or states accountable for an attack.

The fourth and last remaining problem is applying the law itself. Article 2(4) of the United Nations Charter bans the use of force against other states, which is also part of customary law. This law applies to every state regardless of UN membership. Article 2(4) is significant because if a cyber-attack were to be defined by the United Nations as a use of force in the future, the laws applicable to cyber security would set out very different boundaries than if it were not considered to be an act of force. Article 51, however, allows for the self-defense by states that have suffered an armed attack. In order to be able to apply Article 51, there must already be an existing solid definition of what a cyber-attack is and whether it is considered an armed attack or not.

Currently, armed attacks in international law only refer to attacks which are kinetic in nature. Due to cyber attacks' non-kinetic nature, the application of this article would be quite difficult. Kinetic attacks are those which require physical action to hit a target, such as shooting a weapon, dropping bombs, shooting missiles, etc. The same issue can be found in attempting to apply the Laws of Armed Conflict (LOAC) and the Tallinn Manual. The laws governing *jus ad bellum* and *jus in bello* do indeed have the potential to be applicable to hostile cyber operations, but it will be largely up to the United Nations to tackle the issue of definition, as Article 39 of the Charter states that only the United Nations has the authority to name or define an "armed attack" and each attack is subject to different interpretation.

Various scholars have explored the applicability of existing international law to cyber security, and the vast majority of them have come across the same obstacles that I discuss. Shaun Roberts argues that there are five different ways in which the issue with the application of the current law could be tackled (Roberts, 2014). These methods are through an instrument-based approach which would assess the non-traditional nature of weaponry; a target-based approach that would assess who the target is and what the damage is; an effects-based approach that focuses on the effects of the attack itself; a sovereign-based approach that would deem any attack on a sovereign nation as an armed attack; and, lastly, a non-kinetic effects approach that would determine whether the cyber-attack produced a threat to human life (Roberts, 2014).

I will explore Roberts' (2014), Dev's (2015), Clarke's (2010), and Brenner's (2011) suggestions for applying international humanitarian law to cyber security, and I will assess the current and future threats that we face to our own national and international security. As a result, my research method will be in the form of qualitative, secondary data analysis. I will further delve into international law and its ambiguities, how this affects the nature of the cyber threat, and, further, I will explore various scholars' debates on cyber disarmament as a possible solution to this problem in a similar fashion to the way in which nuclear weapons were approached. The main states that will be focused on throughout my study will be China, Russia, Iran, and the United States, as all have already successfully launched one or more cyber-attacks with cyber weapons of high sophistication. I suspect that no matter which direction I take in exploring international law and other scholars' works, I will keep running into the same four obstacles that I outlined in my introduction.

Introduction: The Beginning of a New Era in Modern Warfare

The first major appearance of cyber-security strategies came after the 2007 cyber-attacks in Estonia, in which 500 electronic services and 75 public information state systems were infiltrated by Russian hackers in one of the first large scale DDoS (distributed denial of service) attacks (Patrascu, 2018). In this particular type of cyber-attack, a computer engages in the infection of other computers through what is known as a "worm", and as many as 8,500 computers belonging to innocent people in 178 different countries were infected with malware that was later commanded to inflict the attacks on Estonian infrastructures and cause momentary paralysis of critical systems (Baradaran, Nazanin, Habibi, Homayoun, 2019).

As Shaun Roberts explains, a DDoS is greater in severity than a DoS (denial of service) attack due to the ability of the hacker to “pre-infect” thousands of computers which unknowingly participate in the flooding of critical systems through cyberspace, as was the case in Estonia. A DoS attack prevents the user from being able to access their services, but it is temporary and does not cause such complex flooding of systems (Roberts, 2014). A year later, Russia struck again, but this time against Georgia in the summer of 2008 during the Russian invasion. The purpose of this cyber-attack was to freeze technological networks so that Georgians would not be able to access news or media to get informed on what was going on during the invasion. This marked the very first time that a cyber-attack coincided with a kinetic conflict, and although the cyber-attack was successful to some extent, it was not able to do the same amount of harm that was done to Estonia due to Georgia’s under-developed technological networks (Patrascu, 2018).

One of the most advanced cyber-attacks that we have witnessed thus far was the computer virus named “Stuxnet”, which was used to attack Iran in 2010. The purpose of this cyber-attack was to target and destroy as many Siemens industrial controller nuclear centrifuges as possible in order to severely undermine Iran’s nuclear progress. Stuxnet was a highly sophisticated attack conducted by a team of cyber “warriors” who had very extensive knowledge of how to infiltrate SCADA technology (Supervisory Control and Data Acquisition). SCADA systems are vital to states’ national security, as these systems control things like electrical power grids, oil, gas, nuclear energy and many other crucial systems.

What is most alarming is that states' SCADA systems remain one of the most vulnerable and easy to hack despite massive efforts to strengthen national security and protect them.

The Stuxnet virus remains one of the most complex malwares in the world and has been referred to by some scholars and politicians as the world's "first real cyberweapon" (Berger, 2017). One of the reasons that explains why Stuxnet in particular was such a dangerous and successful virus, is that the method of infection in this particular package of malware was able to replicate itself at extremely high speed and it was also designed to be able to infiltrate systems that were not connected to the internet at all (Berger, 2017). There have been, however, other viruses since then which have also been successful in infiltrating SCADA. In 2016 for example, Iran was able to hack U.S. infrastructure and attack a dam just 25 miles north of New York city. The cyber-attack allowed Iranian hackers to be in full control of the dam and its functions and could have caused great damage. Fortunately, the attack was immediately identified and the controls to the sluice gate were turned offline in order to avoid the potential release of water. In such a dramatic case, international law would have regarded such an event as an attack and the adversary state would have been subjected to an international response.

Some scholars argue that the United States is a glass house when it comes to cyber security, and that although it is able to create cyber weapons of great sophistication it remains nevertheless very weak when it comes to its own defense. Today, there are at least 41 countries that have cyber warfare doctrines and at least 17 of these have offensive cyber weapons and potential (Segal, 2016). Kovacs argues that this number is even higher now, and that in the past 15 years at least 70 states have adopted cyber security strategies

(Kovacs, 2018). Not only have the Russians and Chinese proven that they are capable of hacking into American critical infrastructures, but they have also hacked U.S. military aircraft and other military vehicles (Harris, 2014). This is a clear indicator that cyber security is paramount to all states now, and the race to security is on. Aside from having to worry about adversary states taking advantage of this weakness, non-state actors are slowly catching up and building their own cyber capabilities as well. This equates to a total series of catastrophes in the future if terrorist groups like ISIS gain the technologies to be able to hack into cars and planes for example, or to infiltrate SCADA and critical infrastructures (Govern, Finklestein, 2015). By focusing so much on the applicability of law, however, we may also be making the mistake of not placing enough attention on national cybersecurity efforts. Therefore, it is imperative that the United States focus on protecting itself from attacks first, before anything else.

CHAPTER TWO

Ambiguities in International Law

These events marked a new era in security strategies adopted by states all around the world, as the fear of a highly modernized technological form of warfare became a serious reality and threat. There has not yet, however, been an incident in which a cyber-attack has been referred to as the use of force, and this is because national laws and international law in particular have not been developed to include cyber-attacks as an act of war. Part of the reason why so many ambiguities in international law regarding cyberspace still remain is due to the nature of cyberspace which has not yet been properly defined and thus it becomes very difficult to fit an undefined realm of conflict into already existing legal frameworks (Berger, 2017).

There is much ongoing debate on what constitutes a cyber-attack and if it can even be considered an act of war at all. This is because all currently existing law regarding warfare only deals with kinetic events. Since cyber-attacks are not exactly kinetic in nature, it has been incredibly difficult to apply the LOAC (Law of Armed Conflict) for example, to cyber phenomena. Ashley Berger and various other scholars argue that one way in which a cyber-attack could perhaps be treated as a kinetic attack and thus applicable to existing international law, would be if the cyber-attack leads to any human deaths (Berger, 2017). Heads of state are increasingly worried about the security of critical infrastructures such as electric power grids, which remain terribly vulnerable. If a cyber-attack were to be conducted and was successful in shutting down the electric power grids in Boston in the middle of winter, for example, this could very well result in the deaths of people who have no means to heat their homes and take shelter from the cold. Berger argues that in such circumstances existing law could in the future be applied and a cyber-attack dealt with as if it were indeed an armed attack, and this is where IHL (International Humanitarian Law) comes next (Berger, 2017).

International Humanitarian Law

IHL is comprised of a series of *Opinio Juris* expressions as well as international customary law and treaties such as the Hague Conventions and Geneva that bind states, but the lack of consensus among states regarding cyber related conflict makes it almost impossible for the proper application of existing IHL in response to cyber incidents. IHL primarily deals with the protection of those who are not parties to the conflict such as civilians, as well as the means or methods of warfare which are to be permissible under international law (Ayalew, 2015). It is also up to IHL to determine whether a cyber-attack may or may not reach the threshold of armed conflict (Piatowski, 2017). In the case of a cyber-attack on a power grid that results in the death of civilians, IHL may indeed be applicable in proportionality to the attack.

IHL protects civilians from conflict under international law, and Ayalew argues that this approach may be the best angle from which to tackle issues of ambiguity regarding cyber conflict in legal frameworks. Article 36 of the Additional Protocol I to the 1949 Geneva Convention holds that “In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party" (Ayalew, 2015). This means that there are already legal grounds for states to debate and try to come to some consensus on how the emergence of cyberspace as a new weapon applies to existing IHL.

Bodies of IHL have already successfully created restrictions or prohibitions against certain warfare tactics such as the use of chemical and biological weapons for example, and such ought to be done with cyber-attacks as well. Schmitt and Watts note that although some forms of IHL may already be applicable to cyber-attacks, IHL is based on *opinio juris* (an opinion of law) and this is the remaining component that renders many ambiguities still (Schmitt, Watts, 2014). Furthermore, Ayalew notes that under current law, if a cyber-attack is conducted while an ongoing armed conflict is taking place simultaneously, then existing IHL rules already apply and that the only remaining obstacle in IHL is being able to define and categorize cyber-attacks under the laws of armed conflict so that hostile cyber activity may also be monitored alongside already existing kinetic conflict (Ayalew, 2015).

Article 52(2) of Additional Protocol I to the Geneva Convention asserts that a military attack is only legally permissible against "those objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization offers a definite military advantage" (Pool, 2013). A major obstacle facing the application of these articles of the protocol, is that in order for combatants to be apprehended they must have a thoroughly organized or state command structure of some sort, and this is something that many, if not most non-state hackers do not have, and even if they did, it would be very difficult to prove that there is such a connection between the hacker and a state leader. Nevertheless, the U.N. Charter clarifies that in this case, individuals conducting attacks against another state are to be held responsible under the state in which they were operating. If a supposed non-government affiliated hacker group in China were to attack the United States for example, China would still be held responsible for its citizens who committed the attack.

The largest obstacle to the application of IHL however, remains the issue of definition and *opinio juris.* If a cyber-attack could be categorized as a kinetic attack depending on the damage it has caused, it would have to be regarded as a new domain of warfare, and it would most definitely have to be a conflict occurring between two or more states. Anonymity will continue to be a major challenge, as will attribution and the ever-growing presence of non-state actors conducting attacks for the government through indirect affiliation. Even if these issues were to be resolved, there still remains the issue of the “dual use” concept in IHL. Dual use refers to a means or network that is used both for civilian and military purposes, and once a military uses the same network as civilians, it is regarded in IHL as a lawful military target (Schmitt, 2014). The dilemma here is that most cyber networks and infrastructures have been in dual use for a very long time already and will continue to be this way into the future as well. The same internet traffic used for the military is also used by civilians, and GPS technology, for example, is widely used for both military and civilian purposes and while this continues to be the case, dual use operations will remain lawful ones under IHL (Schmitt, 2014).

The U.N. Charter

The U.N. Charter states that according to Article 51 of the Charter, states are lawfully permitted to respond against an armed attack from another state so long as that response is in proportion with the initial offensive attack (Piatowski, 2017). In theory, then, states ought to be allowed to respond when a cyber-attack is received. This is not yet the case, however, as Article 51 of the Charter only deals with armed attacks in the kinetic, on the ground nature. A major obstacle to the inclusion of the cyber realm in the Charter and other bodies of law still remains, and that is the issue of being able to define whether a cyber-attack can indeed constitute an armed attack or not. It is also still unclear if a cyber-attack may be regarded as employing force or not, and these definitions are absolutely crucial for the successful application of existing international law to cyber-conflict.

Even if the use of force was permitted as a legitimate form of defense against a cyber-attack, the charter does not offer a definition of what the "use of force" means, and the loosely implied characteristics of force are very unclear as a result (Berger, 2017). Another problem is that Article 51 in some ways clashes with Article 2(4), which advises states to refrain from using any type of force against other states unless, as Article 51 declares, it is a matter of self-defense (Berger, 2017). Furthermore, the resolutions of Chapter VII in the U.N. Security Council state that self-defense and retaliation to an attack must be an absolute last resort. The Charter however, still only deals with kinetic armed attacks or the kinetic use of force, leaving great ambiguity when dealing with any sort of cyber-attack or violation. According to the International Court of Justice during the Nicaragua v United

States case, an armed attack is regarded as being most severe when it results in the loss of human life or huge material destruction (Military and Paramilitary Activities in and Against Nicaragua (*Nicar. v. U.S.),* 1986 I.C.J.14, 181 (June27).

Perhaps this is one way in which cyber-attacks may begin to be treated as seriously as kinetic attacks, due to their kinetic destruction as a result of the attack. Perhaps then, until a cyber-attack results in the loss of life or in great material destruction, the qualification of the attack as an armed attack will not be possible (Baradaran, Habibi, 2019). Cyber-attacks make it very difficult for states to be able to apply Article 51 due to the anonymous nature of the attacks as well. In order for a state to invoke Article 51 of the Charter, it must first be able to attribute the attack to the source, and this, in most cases, is an extremely difficult and time-consuming task (Baradaran, Habibi, 2019). According to customary law, attributability is absolutely necessary as a method of international responsibility and accountability.

These specific laws of responsibility are outlined in Article 3 of the Fourth Hague Convention (IV) and also in article 91 of the Protocol Annex I of Responsibility (Baradaran, Nazanin, Habibi, Homayoun, 2019). UN Charter Article 39 may also offer a possible solution in dealing with cyber-attacks due to its statement on the breach of peace:

"The 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 measure shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security" (U.N. Charter, art. 39).

If the U.N. Security Council came to an agreement on cyber security, cyber weapons, and cyber-attacks in the future, it could very well identify a cyber-attack as a breach of the peace and therefore when an attack is committed, it could be treated as a violation of the Charter (Dev, 2015). Under customary law, however, a violation of Article 39 does not yet qualify as an act of unlawfulness because of Article 2(4) in dealing with the use of force, and so applying Article 39 to any kind of attack, kinetic or cyber, would be very difficult (Dev, 2015). Nevertheless, the decision is still at the Security Council's discretion and the members of the Council can decide whether an act may be regarded as an attack, or not. Lastly, there is no definition in the U.N. Charter to define what a breach of peace even is, and this would prove highly problematic even without the impediment of Article 2(4) on the application of Article 39 (Dev, 2015).

Though the U.N. Charter does not provide an actual definition for what an armed attack means, it does have various qualifications which are used to determine if the attack can be deemed an armed attack or not. One of these requirements came as a result of the ICJ *Oil Platforms Case* in 1992, in which the Court concluded that an armed attack must have the specific intent to cause harm (Zemanek, 2013). Whether an attack had the intent to cause harm or not, is something that can only be decided by the Court during a formal judicial proceeding (Zemanek, 2013). In the *Nicaragua v United States of America* case of 1986, the International Court of Justice ruled that there is indeed a difference between attacks that use excessive amounts of force, and attacks that do not, and this distinction is what has also helped international law to more or less be able to determine which kind of attack may be regarded as an armed attack, and which may not (Zemanek, 2013).

In terms of attributability, the Charter primarily focuses on states, leaving substantial gray area with regard to non-state actors that are very loosely affiliated with the government and launch attacks against other states. Article 3 in the Fourth Hague Convention (IV) and Article 91 in Protocol Annex I of Responsibility however, imply that attacks conducted by any belligerent group that has been either trained, controlled, or tolerated by the government are also the state’s responsibility and therefore attribution of individual hacker groups who attack for the state, are subject to international law as well since they would be regarded as being part of the state’s responsibility (Baradaran, Habibi, 2019).

In order for U.N. Charter law to be applicable to the increasing cyber crisis, a definition of cyber-attack and cyber warfare ought to be adopted or recognized by Article 2(4) of the charter so that existing law may be applied to the cyber realm of conflict (Baradaran, Habibi, 2019). When cyberspace is accepted as a new domain of warfare in the U.N. Charter, perhaps Article 51 could be invoked in response to an attack, but until there are clearer definitions outlined in the Charter, it will be very difficult to do so. Once it becomes applicable, rules of proportionality found in Articles 2(4), Article 51(5)(b), and Article 57 may be used in responding to a cyber-attack according to the U.N. Charter law (Pool, 2013).

The Tallinn Manual

The *Tallinn Manual* does encompass cyberspace as a realm of warfare, though not very clearly because it does not set *lex ferenda* (future law or what we want the law to be) or best practice recommendations. The Manual was produced in 2013 by the NATO Cooperative Cyber-defense Centre of Excellence, and in its most basic form, it investigates the application of international law to the field of cyber warfare, "international cyber security law" and "law of cyber armed conflict" (Kovacs, 2018). There are nineteen law expert authors of this manual, and there are two versions. The *Tallinn Manual* 1.0 and the *Tallinn Manual* 2.0. The Tallinn Manual 2.0 was released in 2017, four years after the first manual. For the purpose of international law, the *Tallinn Manual* 2.0 is the most useful because it provides a very comprehensive analysis on how current bodies of international law may be applicable to cyberspace. It is a continuation of the 1.0 Manual, but it is more concrete, precise, and relevant for today's cyber climate (Kovacs, 2018).

According to the *Tallinn Manual*'s definition of armed conflict, cyberspace is included as a realm of warfare and when a cyber-attack occurs, it ought to be regarded as a traditional armed attack (Piatowski, 2017). *The Tallinn Manual* also deals with conflict with armed hostilities, but it does not directly discuss kinetic to cyber-attacks of any kind and this leaves ambiguities in the relationship between a cyber-attack during peacetime, *jus ad bello*, and *jus in bello* (Fleck, 2013). The manual also falls short in making a distinction between non-destructive but severe cyber-attacks and destructive cyber-attacks, and which of these would be enough to raise hostilities to the status of an actual armed attack (Fleck, 2013). This distinction is particularly important, as *jus ad bellum* laws protect states' rights prior to a conflict, and *jus in bello* laws apply only during an armed conflict, and, therefore, until cyber-attacks are separated into some sort of scale of severity, it will be difficult to know which body of law may apply to a particular attack (Fleck, 2013). It may be possible however, to make an analogy in law. This is when there are two or more laws that are similar in nature and are applied together to a specific case. An analogy of law may be used when there has not yet been a case that deals with a particular issue, and in this case, could apply in cases of cyber-attacks.

Moreover, Nguyen argues that even if this distinction is made, "*jus ad bellum* provides little guidance about the legality of a cyber-attack or when such an attack becomes an act of war justifying resort to responsive force" (Nguyen, 2013, pg.2). With regard to the conduct of hostilities, the manual states that the Laws of Armed Conflict (LOAC) do not impede anyone from participating in cyber operations, however; cyber activity will result in legal consequences based on the nature of the attack (Ayalew, 2015). There are also additional consequences for combatants who partake in hostile cyber activities. According to the *Tallinn Manual*, combatants lose their status of combatant immunity and prisoner of war status if they fail to follow the requirements of maintaining that status (Ayalew, 2015).

In other words, if an individual protected under combatant immunity or prisoner of war status took part in hostile cyber operations during a conflict, the protective status would be lost immediately and the individual would become an unprivileged belligerent as a result (Ayalew, 2015). The loss of combatant immunity stems from the Direct Participation in

Hostilities (DPH), which applies the notion of direct participation from Additional Protocol I to cyber war and it deals only with *jus in bello* or active armed conflicts (Turns, 2012). This section of Protocol I of Responsibility is an amendment to the Geneva Convention regarding the protections of victims in international armed conflicts (GeiB, Lahmann, 2012).

According to a new rule of the *Tallinn Manual* added by the International Group of Experts, unlawful cyber activity does not have to be destructive or cause injury for it to be dealt under the law of the affected state and international law in general (Schmitt, 2014). The International Group of Experts is a team which is specialized in analyzing the applicability of law (Schmitt, 2014). The possibility of the prosecution of cybercrimes is further outlined in Rule 2 and Rule 24, but they are not discussed in great detail which still leaves too many ambiguities for it to be applicable to cyber conflict. In accordance with definitions of IHL and the U.N. Charter, an armed attack in the *Tallinn Manual* requires a trans-border element, but does not necessarily need to involve weapons, or at least not those of the traditional kinetic nature (Dev, 2015).

This is because Rule 30 states that an armed attack consists of an attack made on a state and causes either death, damage, injury, or destruction (Dev, 2015). Injury is an extremely flexible term in international law, which can apply to various different situations if used correctly. According to IHL, the cause of injury which results in unnecessary suffering and damage to the environment is part of the protection of civilians as a whole, and civilian property. Here, injury could mean a number of different things because the use of the term is very generic, and therefore states could claim injury after a cyber-attack for example (Ayalew, 2015).

Additionally, comment 9 to Rule 13 stipulates that “the case of actions that do not result in injury, death, damage, or destruction but which otherwise have extensive negative effects” remains “unsettled” in classification (Dev, 2015, pg. 16). There is also a lack of consensus on whether an attack had to have significant intention of harm or not, but the majority agreed that intent to harm was in fact required (Dev, 2015). Whether intention to harm is included in this definition or not, states would still be able to claim injury as a response to an attack through cyberspace, due to the term’s flexibility.

Laws of Armed Conflict

The Laws of Armed Conflict (LOAC) are comprised of the Hague and Geneva Conventions as well as customary international law, other treaties, and case law. Article 41 of the UN Charter lists a series of prohibited measures that are not to be regarded as legitimate use of force strategies and this includes the “complete or partial interruption of telegraphic, radio, and other means of communication” (Kirsch, 2012, pg. 12). A cyber-attack, depending on its severity could most certainly fall under this category and would not necessarily interfere with IHL because it does not account for physical harm caused to noncombatants. However, due to the interconnected nature of computer networks, it would be very easy for an interruption of communication to spill over and affect civilians as well. Therefore, while communication interruptions may not constitute armed attacks according to LOAC, such attacks may still be subject to the Additional Protocol I of the Geneva Conventions.

One of the major challenges in trying to apply LOAC to cyber related conflict, is that LOAC, like many other bodies of domestic and international law, primarily deals with conventional warfare. This puts into question the status of hackers as belligerents or combatants under protected status according to other bodies of international law. The "punishment of aggression" as a result of the International Military Tribunal at Nuremberg after World War II defined these activities "planning, preparation, initiation or waging of a war of aggression" as crimes against peace, and while these concepts have been used to handle state conflict, it would be more difficult to do so with hacker groups for example (Jordan, 2016). Jordan argues that one of the key issues in unconventional warfare is that it makes it easy for hackers or belligerents to hide and conduct their aggression in ways that have not yet been assessed in depth by international law (Jordan, 2016).

The Nuremberg outcome on aggression, for example, though vague in definition, was referring to acts of aggression that do not encompass those experienced today with cyber-attacks or cyber warfare. While LOAC may come short in handling hackers and unconventional combatants, there are other bodies of law that do attribute the acts of de facto organs of state and non-state actors to the state from which they are operating. This attribution, which will be discussed in greater detail in a later section, makes the state responsible for those who have committed hacks against other states.

The Law of War Manual

The Department of Defense Law of War Manual, published in 2016, provides guidelines on how to handle armed conflict, how the conflict ought to be assessed, and how it may be treated during times of either war or peace. The Manual, however, does not yet include cyberspace as a realm of warfare and for U.S. national security this continues to be a challenge and obstacle (Berger, 2017). It is not yet clear whether cyber-attacks can be treated as acts of war or not, and this also limits the U.S.'s available retaliatory response as a result. Currently, the manual holds that if a cyber-attack were to in any way resemble the nature of a kinetic attack (i.e. causing loss of human life or severe damage of property), then it would treat the attack as an "armed attack" and enforce all of the retaliatory proceedings already outlined for dealing with a kinetic attack (Berger, 2017).

The International Court of Justice (ICJ) asserts that an armed attack committed by state actors, which in turn creates the possibility of a vacuum for non-state actors to perform armed attacks for the state in a way that would not exactly implicate the state as being responsible for the attacks (Roberts, 2014). The fact that there is little existing law that deals with cyber security at all is of great concern, but it is even more concerning that the efforts to apply international law to the cyber realm are currently only being focused on states rather than both states and non-state actors. There are of course, even more complications in applying law to non-state actors and perhaps law will be able to evolve to encompass non-state actors once law between states has been established.

The Martens Clause

The Martens Clause is a component of LOAC and IHL that since 1899 has only dealt with law regarding conflict on land but has since been recently expanding to try and encompass the cyber realm. The Clause was encompassed in Article 1(2) Protocol to the Geneva Convention in 1949, as the foundation of international humanitarian and human rights law which sets out protections to groups and individuals during both times of peace and times of conflict (Salter, 2012). Among these protections, include the "principles of distinction, prohibition of indiscriminate attacks, the requirement of proportionality in attack, military necessity and prohibition on causing unnecessary suffering" (Salter, 2012, pp. 406).

These components of law, however, though they were created in a time that only encompassed traditional aspects of warfare, may still be applicable to cyberspace conflict. The biggest challenge in using the Martens Clause in IHL is that there is no one single accepted interpretation of the Clause, which creates a lot of ambiguity in terms of how specific or broad the terms and conditions in the clause may actually be applied. Though the Clause does indeed have *jus cogens* (international norm) status in customary and treaty law, the clause remains primarily a judicial guideline, which makes its application in certain cases difficult. Especially regarding new forms of warfare such as cyber warfare, which the clause has not dealt with before.

It is important to note, however, that the Martens Clause does in some cases give the authority to judges to be able to extend current legal provisions to illegal activity that does more than just put the lives of civilians at risk (Salter, 2012). The only problem is that even this authorization lacks guidelines and instructions on how to proceed, especially in a situation in which many aspects of an attack have not yet been defined. Despite its limitations, the Martens Clause remains a relevant component of international law because it makes clear that new weapons ought to be used only with the consent of the international community and that they must at the same time be consistent with International Humanitarian Law (Woltag, 2015).

It is therefore of imperative importance that the international community hastens the conversation on the role of cyber weapons and whether they ought to be permitted, regulated, or completely unregulated. Different states have different interpretations of the Martens Clause, as with much of international law, and without some sort of consensus on basic terms among the international community it will be very difficult to tackle cybersecurity issues.

CHAPTER THREE

The Hacked World Order

One of the most pressing concerns in cyber security right now is the security of SCADA and critical infrastructure systems. These remain some of the most vulnerable systems, and successful criminal infiltration could not only be catastrophic for the continued functioning of the state and military but could also potentially lead to civilian deaths. Iran has proven capable of hacking a dam in New York, and both Russia and Iran have proven capable of hacking U.S. electric power grids. If during a cyber-attack, the electric power grid were successfully infiltrated and shut down, even if just momentarily, in any given location, it could very well lead to the harm or even fatality of civilians. China, Russia and Iran are discussed as being great cyber powers in the world today, and North Korean cyber power is analyzed as well given the country's alliances and its cyber capabilities in attacking the United States.

China

As early as 2003, the PRC (People's Republic of China) created various cyber warfare units at Hainan Island's naval base, and it was here that some of the most sophisticated cyber weapons we have ever encountered were created. Some of these highly sophisticated cyber weapons include information mines (theft of victim's information when encountered), network spy stations (infiltrated systems), clone information (stolen and replicated information), information bombs (set out malicious attacks when encountered by victim), information deception (manipulated information) and many more (Clarke, 2010). Chinese cyber-attacks began with spear phishing emails which released a Remote

Access Trojan (RAT) which allowed the hackers to roam around networks and have easy access to any desired data (Kaplan, 2016). There were also various websites such as chinahacker.com and cnhacker.com that were used to teach people hacking skills and that the main target in these attacks ought to be the United States, due to its “evil” way of life (Govern, Kevin, Finklestein, Claire, 2015).

Prior to these developments in the early 2000s, China had already proven its cyber might in 1999 when it responded to the U.S. bombing of a Chinese embassy in Yugoslavia by conducting a mass cyber-attack which targeted and infiltrated the U.S. Department of Energy, the Department of Interior, and the National Park Services (Harris, 2014). Today, the Chinese military cyber forces are so large that even if they stopped growing right now, they would still be at least five times larger than the cyber forces of the United States (Harris, 2014). This however, does not necessarily equate to capability and does not mean that China would be successful in deploying those weapons. Gertz argues that most of China’s cyber power development comes from within the People’s Liberation Army (PLA)’s Third Department of the General Staff, which is also known as 3PLA (Gertz, 2017). It is currently estimated by American intelligence agencies that 3PLA consists of at least 100,000 cyber warfare troops, and this number is still growing (Gertz, 2017).

Gertz states that the 3PLA’s cyber warriors are highly skilled and trained in code breaking, generating attacks, and foreign languages and that apart from the 3PLA there is also another cyber unit within China’s Fourth Department known as the 2PLA, which is a separate military intelligence unit specialized in electronic warfare and espionage (Gertz, 2017).

Furthermore, a report from the FBI states that aside from the PLA's specialized cyber units, it also has 30,000 cyber spies and 150,000 cyber experts whose sole mission is to launch offensives to steal information from the American government (Brenner, 2011). The PRC has also established spy networks in Cuba which allows the Chinese to monitor U.S. internet traffic as well as DoD communications.

This development led to one of the worst cases of cyber espionage against the United States, known as Titan Rain, in which the Defense Information Systems Agency, Redstone Arsenal, Army Space and Strategic Defense Command systems were infiltrated (Brenner, 2011). In this attack, the Chinese were able to extract 10 to 20 terabytes of Data from the Pentagon's unclassified network as well as 2 terabytes from the Defense Department (Clarke, 2010). Titan Rain was discovered in 2005, but it had been hiding in the system since 2003, which is why it was able to extract so much information.

In 2009 and 2010, the PRC conducted a mass series of cyber-attacks known as "Operation Aurora" against various U.S. companies such as Google, Yahoo, Adobe, and many more although the attacks mainly targeted Google. This is because one of China's goals by hacking Google was to spy on Chinese human rights activists' emails and censor what Google content may be viewed by Chinese people (Harris, 2014).

Another reason why the PRC sought to infiltrate Google was because it wanted to eliminate the visibility of Chinese military facilities on Google Maps (Sanger, 2018). The breach also revealed the names of Chinese intelligence operatives in the United States who were under surveillance and whose emails may have been subjected to espionage by the NSA in a joint agreement with Google.

After this event, the Obama administration adopted a harsher tone with China even though the Chinese outright denied that the attack had come from China at all. Additionally, Google formed an alliance with the NSA so that it could help Google better protect its networks from further attacks (Harris, 2014). In 2013, a threat within U.S. cyber space was identified by the Mandiant (espionage unit) Report, which revealed that an APT1 (Advanced Persistent Threat 1) intruder had been inside the network completely undetected for as many as 1,764 days and that it had managed to steal hundreds of terabytes of information from as many as 141 different organizations and 20 industry sectors (Govern, Finklestein, 2015). An advanced persistent threat is an attack that remains a threat for a very long time and does not easily go away. Additionally, this cyber unit had swiftly established almost 1,000 command and control servers in 13 different countries, including 109 in the United States (Govern, Finklestein, 2015).

The Mandiant Report also discovered several cyber units called 5138, 61398, and 61486 (also known as Putter Panda) from the PLA that had also infiltrated U.S. networks and stolen information (Govern, Finklestein, 2015). In 2011, McAfee discovered a new Chinese hacker operation named “Night Dragon” which had remained undetected in inside U.S. energy companies for up to four years. Before being found out, however, the hackers conducted an attack to steal as much last-minute SCADA information as possible (Govern, Finklestein, 2015). These attacks were sophisticated in nature, but the attacks themselves were conducted in a very sloppy manner which left plenty of evidence to successfully attribute the attack to a town named Heze in Shandong Province, China (Govern, Finklestein, 2015). This is significant, because it allowed the United States to identify Chinese hacking patterns within its networks, that allow intelligence groups to better identify them in the future as well.

Although there was no significant kinetic damage done, this was an alarming incident for American national security due to the advanced technology used in the attack. Aside from these professional military hacker groups, the Chinese government has also encouraged the creation of citizen hacker groups to engage in espionage of U.S. networks and to lace U.S. infrastructure with logic bombs that can be used at any time (Clarke, 2010). These groups of civilian hackers may pose further complications in the application of international law to cybercrimes, cyber warfare and cyber-attacks because most bodies of law regarding any sort of conflict, are made to apply only in state-to-state conflict and not state-to-non-state conflict. Even though US intelligence was able to get a photo of a prominent PLA hacker who went under the name UglyGorilla and wanted to charge him with cyber espionage, but failed (Govern, Finklestein, 2015).

The Chinese probably already know this, which may be precisely why they are investing so many resources in these groups. Having thousands of different hacker units also helps to create confusion in the aftermath of an attack when states try to attribute the attack to a particular source. It is already very difficult to identify where an attack originated, but it is even more difficult to identify an attack when it comes from thousands of different sources.

Even when attacks are clearly attributable to the Chinese government, however, there has been a lot of reluctance by the U.S. government to call out these attacks and blame the Chinese state for cyber espionage and cyber-attacks on American networks. This is because the economic relationship between the United States and China is important to the stability and development of the American economy and thus the possibility of angering the Chinese and being subjected to sanctions of some sort has been a real concern (Brenner, 2011).

The same principle applies to the Chinese government in some ways. Although the Chinese have no trouble in calling out perceived American cyber-attacks, Harris argues that China has little interest in conducting cyber-attacks that would in any way harm critical American infrastructure because the U.S. is one of China's largest foreign lenders and trading partners and so we should not expect the Chinese to cause a blackout in American power grids for example (Harris, 2014). Currently, U.S. intelligence officials do not rank China as the number one threat in cyber security primarily for those reasons, and because China has not yet conducted a cyber-attack that served as a warning to Americans about the security of power grids, critical infrastructures, or SCADA systems (Harris, 2014).

China has for the most part, engaged in hacking with the purpose of espionage which could also be considered a crime, but it has never delivered an attack to freeze operations or functions in the United States. For the Chinese, Gertz argues that cyber warfare encompasses six components: obtaining information, analyzing and verifying information, protecting information from attack or theft, using information for military purposes, protecting its own information from the enemy, and managing information (Gertz, 2017).

Both the United States and China's disagreements in the cyber realm tend to focus on "the legitimacy of the use of cyberspace for economic or industrial espionage; national security uses of cyberspace for more traditional forms of espionage and intelligence gathering; the prospective use of cyberspace for military operations; the putative rights of states to control information access within their borders; and the issue of how international norms, rules, and the physical architecture of the Internet should be governed" (Harold, Libicki, & Cevallos, 2016, pp. 6). Until international norms and laws have been introduced, it is very likely that these disagreements will persist.

It is estimated by the former director of the NSA that China steals intellectual property from the United States worth at least $300 billion annually, mostly from corporations (Harold, Libicki, & Cevallos). One of the most serious concerns of the United States regarding Chinese espionage today is related to Huawei products, which have been accused of containing undisclosed technology that has allowed for the PRC to spy not only on its own citizens but most importantly on everybody else who possesses a Huawei phone, laptop, or USB (Sanger, 2018). Since the beginning of 2019, Donald Trump has restricted Huawei from being able to enter into contracts with U.S. companies to sell its products, on suspicions of espionage and the threat that those products pose to national security (Sanger, 2018).

Trump was able to do this through executive order #13886 in May of 2019, which basically bans the Chinese from being able to sell Huawei products in the United States. What is of even more concern, however, is the current NSA director's assessment of Chinese activity in other networks that are not related to the theft of business information. Michael S. Rogers recently stated that China has in fact already penetrated our power grids and that Chinese hackers have successfully implanted *back doors* that remain dormant in the network until the hackers decide to use them to wreak havoc (Harold, Libicki, & Cevallos, 2016). Therefore, despite efforts to halt Chinese espionage and intrusion, such acts have been very difficult to control.

Iran

When it comes to cyber threats against the United States, Iran has undoubtedly been one of the key concerns for national security. Like China, Iran possesses very sophisticated cyber weapons that are capable of infiltrating SCADA and critical infrastructures, posing a great threat not only to the security of American intelligence but also to civilians who may suffer from the cyber-attacks as well. Direct attacks from Iran against the United States include the targeting of government personnel involved in non-proliferation issues in 2011, the DDOs attacks on US banks in 2012, the hacking of the Navy Marine Corps intranet in 2012, renewed attacks on US banks in the same year, wiper malware attacks on the Las Vegas Sands corporation in 2014, Operation Cleaver in 2014, and the hacking of the Bowman Dam in New York in 2016 (Gertz, 2017). Two key Iranian hacker groups have since been identified, and they are the ITSec Team and the Mersad Company, both of which have performed cyber-attacks on behalf of the Iranian government (Gertz, 2017).

The fact that Iran was able to hack a dam in New York in 2016, highlights not only a major threat to the United States but also that American cyber security is not as secure as it should be. A key event that still shapes American Iranian cyber hostilities is the Stuxnet virus which was discovered in the nuclear facilities of Natanz, Iran. During this attack known as Operation Olympic Games, the NSA and Israeli cyber unit 8200 were able to hack into the nuclear valves through which uranium gas flowed and then infiltrate the frequency converters which were in control of how fast the centrifuges rotated (Kaplan, 2016).

The normal speed of rotation for these nuclear centrifuges is between 800-1,200 cycles per second and through successful infiltration from the Stuxnet virus, those cycles were manipulated and sped up to 1,410 cycles per second, which inevitably caused the centrifuges to fly apart and become irreparable (Kaplan, 2016). In order for Iranian scientists to not notice what was going on, the Stuxnet virus manipulated the data of the system's monitors to make it look like the centrifuges were working perfectly well, when in fact they were not. This gave Stuxnet more time to cause further destruction while it remained undetected (Kaplan, 2016). Before stuxnet was discovered by the Iranians, the virus had managed to destroy over a quarter of Iran's nuclear centrifuges, basically setting the nuclear facility about 20 years behind in progress (Kaplan, 2016).

Though Iran had conducted various successful cyber-attacks on the United States prior to Stuxnet, the discovery of this American infiltration of their nuclear facility in fact led to the Iranians developing their very own official cyber units which today are growing in number and in sophistication. This necessity of these cyber units was stressed even more after Iran was attacked by a U.S.-led virus again in 2012 called Flame. The Flame virus consisted of multipurpose malware similar to that of Stuxnet and was used to wipe out almost every single hard drive both at Iran’s oil ministry and the Iranian National Oil Company (Kaplan, 2016). As a response to this attack, Iran created its own virus named Shamoon which attacked the joint U.S.-Saudi oil company, Aramco and wiped out 30,000 of its hard drives and planted the image of a burning American flag on every single computer at Aramco (Kaplan, 2016). The attack was very strategic, as it was made on a holy day in Saudi Arabia which meant that as many as 55,000 employees were not at work that day (Govern, Kevin, Finklestein, Claire, 2015).

The Iranian attack on Aramco destroyed 35,000 workstations, three quarters of the company’s computers, and destroyed so much of its technology that it basically sent Aramco back to the 1970s in terms of information technology sophistication (Govern, Finklestein, 2015). Later that year, Iranian hackers also breached Bank of America, JPMorgan Chase as well as the New York Stock Exchange. By December of 2012, Iran had hacked all of the major banks in the United States (Govern, Finklestein, 2015). These attacks used a highly sophisticated DDoS extension named “ItsOKNoProblemBro” which specialized in remaining undetected for sufficient time to ensure maximum infiltration and information theft (Govern, Finklestein, 2015). Another response attack from Iran was cyber-attacks launched on the Las Vegas Sands corporation in 2014, in which $40 million worth of damage was caused, the computers were destroyed and most of the data of the company was stolen. This particular company was targeted because of its owner, Sheldon Adelson, who is a strong advocate and defender of Israel (Gertz, 2017).

The two American cyber-attacks on Iran are significant to today's cyber security and future cyber warfare discussion due to the very nature of the attacks. The viruses were created as a part of the American security agenda and was deemed necessary due to the threat of Iran's growing nuclear power. The NSA responded to a perceived threat through non-kinetic cyber strategies, to cause kinetic damage that would minimize the size of the threat temporarily. This nuclear situation worried the U.S. because of fear of either a domino scenario in the Middle East, or a serious threat posed to Israel, the U.S.'s strongest ally in the Middle East. Iranian oil, on the other hand, is not perceived as a threat to the United States, but due to the American relationship with Saudi Arabia and the fact that Saudi Arabia and Iran are in great conflict over oil production, it is an Achilles heel that was targeted more to make a statement rather than to eliminate any sort of threat.

In other words, the nature of these attacks is not like that of most cyber-attacks that have been witnessed thus far. Both the Stuxnet and Flame viruses had severe economic consequences for Iran, which really crippled the state. These attacks are a potential window into how future conflicts may be fought, rather than through the traditional kinetic forms of warfare with on the ground soldiers and military. Clarke notes that "states rarely attack in cyberspace, but they almost always spy" (Clarke, 2010, pg.141), and they both have drastically different sets of potential consequences.

Russia

The 2007 Russian DDoS attacks on Estonia were a landmark moment in international responses towards cyber threats, as NATO, the European Union, and the United States immediately sought strategies and law to strengthen national security and protection mechanisms to avoid becoming victims of similar attacks. NATO's response for example, was to create a cyber defense center in Estonia in 2008 that would not only serve to further protect Estonia from Russian attacks but potentially to help protect other NATO member states as well (Clarke, 2010). Though the DDoS cyber weapon used on Estonia in 2007 was not very powerful, it was at the very least successful in jamming Estonian systems and halt them from working for a certain period of time (Clarke, 2010).

A similar DDoS weapon was used during the Russian invasion of Georgia, which caused a total media blackout that prevented anybody in Georgia from knowing what was going on during the invasion. The Georgian government's operations were also infiltrated and jammed, so that they could not provide any response to the invasion. Though cyber anonymity is still a hindrance in holding attackers accountable, in this case it was found that the attacks all came from the Russian intelligence apparatus, but the Kremlin denied that this was true and instead blamed fanatic patriots, knowing very well that accountability with non-state actors in international law is even more complex (Clarke, 2010). This incident occurred again in 2014 with the Russian invasion of the Crimea in the Ukraine. During the invasion, Russian hackers jammed Ukrainian infrastructure and communication systems with over 6,500 attacks in just two months (Sanger, 2018).

An attack against the U.S. occurred in 2008 when a USB containing viruses and malware from Russia somehow made its way into a US military base in the Middle East. The USB was found in a parking lot at the military base and was later plugged in to one of the base's computers. Once plugged in, the computer became infected with SPIRnet malware and this allowed Russian hackers access into the Pentagon’s networks (Sanger, 2018). During this period, Russian hackers mostly conducted spear phishing attacks which consist of the attack and infiltration of many different accounts or groups, to find as many entry points as possible (Watts, 2018). It was not until 2016 that Russian advanced persistent threats (APTs) would be capable of “whale phishing”.

By 2010, a series of analyses concluded that Russia accounted for about one third of the world’s cyber-crime revenue which amounted to a whopping $3.7 billion annually (Governor, Finklestein, 2015). In the same year, Russian hackers got into the Nasdaq stock exchange with a digital bomb that had the potential to freeze the stock market’s computers and basically wreak havoc on the American economy (Governor, Finklestein, 2015). Fortunately, this digital bomb was never detonated because it was discovered in time, and thus the Russians were not able to harm Nasdaq or the economy. Nevertheless, the fact that Russian hackers were able to breach these networks and successfully plant digital bombs is very concerning and poses a great threat to the future of the economy and the security of such infrastructures (Governor, Finklestein, 2015).

The following year, a Russian P2P (peer-to-peer) malware led by a hacker named Slavik was discovered after many people fell victim to theft of their banking information which completely wiped out their bank accounts. The sole purpose of this malware named GameOver Zeus was simply to steal as much money as possible from as many people around the world as possible and it was successful in doing so for quite some time before it was discovered. Slavik then later developed CryptoLocker malware that infected computers and then encrypted their information which would only be released back to its owner in exchange for money. This sort of attack is known as a ransomware attack, and it is becoming a growing concern in the cyber security of individuals today.

Since these events, Russian Advanced Persistent Threats (APTs) have developed great sophistication and today encompass a wide range of different forms of cyber-attack techniques and the most commonly used variant up to date is a malware known as “Zero Days” (Watts, 2018). These APTs have gone under the code names of APT28 (Fancy Bear) and APT29 (Cozy Bear), both of which are comprised of different competing hacker groups seeking to hack adversary networks to conduct cyber espionage and information theft from heads of state and high ranking military personnel, a technique otherwise known as “whale phishing” (Watts, 2018). One of the biggest “whales” to be phished by these APTs was John Podesta, Hillary Clinton’s campaign manager (Watts, 2018).

The most serious threat and violation of American democracy through cyberspace came in 2016 when the Kremlin successfully hacked the U.S. presidential elections through the use of Cozy Bear and Fancy Bear. Using a specialized Russian military hacker named Guccifer 2.0, Russia released 20,000 classified documents from the Democratic National Committee and revealed information that the DNC used various tactics to push Senator Bernie Sanders out of the race, making Hillary Clinton the front runner in the race for president (Gertz, 2017). Revealing this information made many Americans who supported Sanders extremely upset, and as a result many elected not to support the only remaining democratic candidate as a form of protest (Gertz, 2017).

The breach of the American presidential elections took place because Fancy Bear and Cozy Bear were able to remain completely undetected inside the DNC networks since 2015, gathering information on communications, strategies, and emails. These APTs were only discovered after the DNC hired a private cyber security firm called Crowdstrike to conduct an investigation (Fuller, 2019). One key element of this hack that was instrumental in the destruction of Clinton's campaign was the release of her emails containing classified information which she had sent from a private email account instead of her official government account. As soon as this information was released to the media, it caused mass discontent and suspicion of Hillary Clinton's behavior and intentions in using this private email account. She would not have been, however, the first American head of state to use private emails prior to or even during their presidency but this minor detail did not seem to matter to the public.

Aside from the mass theft of information, internet bots (robots that run automated tasks upon command) were also installed to promote the hashtags "Behngazi", "Trump", "crooked Hillary", "lock her up", "emails" among many others, and through the grandeur of this spamming campaign, these hashtags became trending topics on Twitter, Google, and other social networks and social media (Watts, 2018). With the release of this information and that of Bernie Sanders' suppression by the DNC, Hillary Clinton's campaign was severely damaged, and the Russians succeeded in making Donald Trump the winner of the presidential race. Watts argues that "the Russians didn't have to hack election machines, they hacked American minds. The Kremlin didn’t change votes; it won them” (Watts, 2018, pg. 156). This is the very scary reality that we now face in the securitization of cyberspace, and it will undoubtedly be a challenge again in the upcoming elections of 2020.

The world is so interconnected today and so many Americans get their news and information from social networks, that this has created an enormous vulnerability from foreign influence or “fake news” that Americans unknowingly consume (Watts, 2018). Watts found that the topic of Clinton’s emails alone was a subject of over 65,000 sentences which is double the amount of sentences of a specific topic that has ever been used in any presidential campaign in history (Watts, 2018). The fact that this topic was so heavily emphasized by Russian bots in social networks and social media, diverted Americans’ attention from any of the Trump scandals that had already been revealed as well. Suddenly, the American population was more concerned about Hillary Clinton’s emails than they were about Trump’s grossly racist, misogynist, violent remarks. Because of this, Watts argues that the threat to American democracy does not really come from Russia but rather from the American people themselves because they so easily became “clickbait” to populism (Watts, 2018).

This argument is missing some evidence, because had it not been for Russian APTs, the American people would not have been swayed nor manipulated the way that they were. The state should also take this experience into account and learn to educate the public on how to spot fake news, and how to use social media and networks in a safe manner that will not lead them to be manipulated by foreign actors. It is after all, the state's duty to protect its citizens under international law and in this new age of cyber insecurity, cyber threats ought to be taken into account as well because the power of information warfare can make people think and do things that can put fellow citizens at risk, as well as the state itself.

The Russians mastered the art of deception through fake news a very long time ago, and in fact, a report from the CIA Open Source Center has found that Russia's Foreign Intelligence Service (SVR) has been increasing the development of blogs, websites, and social media tactics to sway public opinion regarding many different issues (Gertz, 2017). Additionally, Russia spends about $500 million a year in disinformation warfare and internet trolls, a strategy which Trump began using at the beginning of his campaign as well (Gertz, 2017).

North Korea

North Korea has proven that its cyber weapons are sophisticated enough to hack into large American corporations, as it did in 2014 with the hacking of Sony. Prior to the Sony hack however, North Korea had shown that it was developing sophisticated cyber skills when they successfully hacked a TV channel in the United Kingdom called "Channel 4" to try and steal or delete a new fictional British TV series that was about an American president and a British prime minister who collaborated to free a nuclear scientist who had been kidnapped in Pyongyang (Sanger, 2018). The North Koreans clearly did not like this representation of North Korea in western media, and so it sought to damage Channel 4 and the series as revenge. Fortunately, the cyber-attack was detected by British intelligence before any serious damage was done (Sanger, 2018).

North Korea hacked Sony specifically due to the production of the American comedy movie called “The Interview” (2014) which depicts Kim Jong Un’s assassination. Right before the movie was going to be released, North Korea hacked Sony and said that if the movie were released to the public, there would be another September 11th scenario in the United States (Segal, 2016). This caused a lot of discussion in the U.S., as people were afraid that the threats may be legitimate and that the release of this movie could be an actual potential threat. The Obama administration took time to decide how to proceed and ended up deciding that no foreign state should have the power to dictate how our American democracy is run. Nor, should we be made to fear for simply releasing and watching a movie.

“The Interview” (2014) ended up being released to the public and nothing happened as a result. There were no attacks from North Korea, and the infiltration of Sony was also dealt with accordingly. This does not mean however, that North Korea may not be a serious cyber threat in the future. Various defectors from North Korea have claimed that the government and military in North Korea are building cyber armies full of young people who have been highly trained to infiltrate systems and conduct attacks (Segal, 2016). There are also serious economic consequences that come with these attacks that ought to be taken into consideration as well. The Sony hacks alone cost over $35 million in damages, and if such attacks were to happen, American firms could be at serious risk (Segal, 2016).

After the attacks, the U.S. government asked China for help to deter North Korea in its cyber operations but the Chinese simply responded by arguing that there was no real proof that it was North Korea that was behind these attacks, as the IP addresses related to the attack generally came from Thailand, Bolivia, Singapore, Cyprus, and even the United States (Segal, 2016). U.S. intelligence was able to attribute the attacks to North Korea because the North Korean hackers forgot to use proxy servers that would hide their identities, and this is how they were found out. Had the North Koreans not made this mistake, it would have been even more difficult for the U.S. to be able to successfully attribute the attack.

The reluctance of the Chinese to offer help in this regard, raises questions about where such high cyber sophistication in North Korea originated. China remains North Korea's largest trading partner, and despite North Korea's nuclear and cyber developments, China remains silent and refuses to condemn Kim Jong Un (Sanger, 2018). Gertz also criticizes the United States for the lack of serious action that was taken in dealing with North Korea in response to the cyber-attacks against Sony, but there currently are not enough legal means which the United States could have employed to deal with this problem, and this is precisely why the development of international law ought to be one of the primary concerns when dealing with cyber security (Gertz, 2017).

De Facto Organs of a State and State Responsibility for Private Actors

International law does not generally hold states accountable for the actions of private actors, but there are a few exceptions in which states are indeed held accountable depending on the acts committed by the private actors, whether they are individuals or de facto organs of state. The concept of *due diligence* or violation of a norm in international law is what is examined in order to make an attribution linking the state and the private actor (Kees, 2011).Though there is no clear path in international law to attribute individuals or de facto organs of state to the state, there have been significant efforts to do so and these are the legal foundations which will be of crucial importance to holding states accountable for hacker groups or individuals who do not directly work on behalf of the state but who conduct attacks for the state.

The concept of de facto organs and individuals of state is usually first dealt with under the umbrella of international law rather than municipal law (Palchetti, 2017). According to the International Law Commission (ILC), "in exceptional circumstances, functions may be considered as given to an organ or agent even if this could not be said to be based on the rules of the organization" (UN ILC 'Text of the Draft Articles with Commentaries Thereto: Responsibility of the International Organizations' [2011] GAOR 66th Session Supp 10, 69). Considering that it is not a simple task to attribute a group or an individual to a state, there still remains the *Responsibility of States for Private Actors* principle which lay out legal consequences to the state for the actions of its citizens (Palchetti, 2017).

This decision came out of the Nicaragua v United States of America case, in which the International Court of Justice (ICJ) stated that since the United States did in fact take part in the financing and training of the *contras,* it was therefore responsible not only for its own conduct within Nicaragua but also for the conduct that could be related to the *contras* themselves too ([1986] ICJ Rep. 65). Furthermore, the ICJ held that the U.S. violated international law as well as principles of customary international law due to its involvement with the *contras* and this is what set the legal framework for the attribution of de facto organs of state to the state which in turn translate to state responsibility (Palchetti, 2017).

Additionally, in order to make the attribution, it must be found that the activities of organized military groups that are controlled by the state directly or indirectly have indeed been subjected to the control of the state as was the case in Nicaragua v United States of America (Palchetti, 2017).

The ICJ also found that:

> "The secrecy in which some of the conduct attributed to one or other of the Parties has been carried on **. . .** makes it more difficult for the Court not only to decide on the imputability of the facts, but also to establish what are the facts. Sometimes there is no question **. . .** that an act was done, but there are conflicting reports, or a lack of evidence, as to who did it. The problem is then not **...** imputing the act to a particular State for the purpose of establishing responsibility, but tracing material proof of the identity of the perpetrator." (Jordan, 2016).

This statement highlights the issue of identifying the aggressor when they hide their actions during a conflict, which is very easy to do through cyber networks. Despite the fact that in the *Nicaragua case* the United States accused Nicaragua of giving cross- border sanctuary to belligerents, supplies, and support to groups in El Salvador, the ICJ was nevertheless still unable to make a direct connection between the insurgent groups in El Salvador and the Nicaraguan government (Jordan, 2016). Although there was evidence to hold the Nicaraguan government accountable for the support of insurgents in El Salvador, there was simply not enough concrete evidence in order for the case to have a different outcome and that is why Nicaragua was not held accountable (Jordan, 2016). This is perhaps something that will be an issue in dealing with hackers and conflict through cyberspace as well.

According to Article 4(2) of *Articles on State Responsibility*, "an organ includes any person or entity which has that status in accordance with the internal laws of the state", which means that even if the individual does not have a formal status under municipal law, they may still be treated as organs during the attribution stage depending on the role they played in the structure of the state itself (Palchetti,2017). Complementing Article 4(2), Article 9 of the *Articles on State Responsibility* also asserts that attribution may occur when an individual "exercises elements of governmental authority in the absence or default of the official authorities of the state" (Palchetti, 2017).

Article 8 of the *Articles on State Responsibility* is particularly important in the determination of individual or de facto group actions operating under state orchestrated instruction and direction, which reflects customary international law and can therefore lead to applied attribution to a particular state (Kees, 2011). These concepts have already been applied in several cases after the *Nicaragua v United States of America* case, but the challenge now will be to apply this existing law to cyber conflict. Hacker groups and individual hackers, as discussed throughout the paper, are extremely difficult to track down and pinpoint to a specific state due to the use of stolen IP addresses or mass infection of thousands of computers all around the world all conducting the same attacks simultaneously.

Therefore, we find ourselves in a much larger problem. Legal frameworks to attribute de facto organs of a state and private actors may exist and have proven successful in the past, but we are yet to see a case in which the *Articles on State Responsibility* can be adequately applied to actors who are almost impossible to track down and locate accurately. International law may only be applied when a state is certain that the attribution being made is absolutely correct without flaw, and the applicability of this with regard to cyber criminals is becoming increasingly difficult. In order to tackle this issue and be able to use existing law to hold states and non-state actors accountable for attacks, our technology must have the capacity to accurately identify the hackers and where they are attacking from.

Another major obstacle faced in the *Nicaragua* case was that the insurgent groups were operating from the other side of an international border and could therefore not be directly attributed to the Nicaraguan government. This will be a major issue in handling cyber-attacks, because in most cases, attacks do not come from one source or one launching site but rather, many. The hacker may not even be in the same country from which the attack is launched, and this is a huge problem in being able to apply the bodies of international law. Even if hackers did stay in one location, they are still able to hide and manipulate the visibility of their location with proxy networks, VPNs, and false IP addresses (Jordan, 2016). Even if an attack could be attributed to a source or one single computer, this still does not provide evidence about who was behind the computer at the time of the attack (Jordan, 2016). In order for this to change, LOAC ought to be expanded to encompass cyberspace as a legitimate realm in warfare today.

Armed Attack by a Non-State Actor

According to the ICJ decision in the *Nicaragua v United States* case, an "armed attack" can indeed be committed by unconventional groups. However, there is no clear definition of what this armed attack would consist of, nor who unconventional groups really refer to. Nevertheless, this gray area could also be seen as an area of legal flexibility and made quite useful. Whether an attack committed by non-state actor groups can be regarded as an "armed attack" under the U.N. Charter Article 51's requirements, is still subject to much debate. Some argue that the attacks of 9/11 for example, ought to be treated as an armed attack by a non-state terrorist organization (Zemanek, 2013). If a cyber-attack were able to have consequences of the magnitude of 9/11, would it be considered an "armed attack" under Article 51's parameters? After 9/11, a US Representative to the U.N. Security Council argued that such an attack falls under Article 51 and that therefore the United States has every right to retaliate to the attack with the use of force (Zemanek, 2013). Additionally, Article 5 of the *NATO Treaty* was also used to declare the events of 9/11 as an armed attack, and NATO does have the power to declare a cyber catastrophe an armed attack as well.

The Security Council accepted this statement and backed its argument by adopting two resolutions. The first is Resolution 1368, which was created in 2001 and accepted unanimously in the Security Council. Resolution 1368 is dedicated to fighting against international threats to peace, through the cooperation of UN Security Council member states in a joint effort. Resolution 1373 was also adopted unanimously in 2001 under Chapter VII of the United Nations Charter, and it binds all U.N. member states (Zemanek, 2013). Resolution 1373 deals with terrorism specifically and required states to amend their domestic laws so that the principles of the *International Convention on Terrorism* could be adequately applied and executed by all member states (Zemanek, 2013). These principles include measures such as background checks on asylum seekers before they are granted asylum, regulating immigration, etc.

Unfortunately, however, this resolution failed due to the U.N. member states and the U.N. Security Council's inability to define terrorism. Again, we find ourselves in a situation in which great efforts in international law have been made in order to tackle a particular problem, but defining these problems is an extremely complicated task. This could have alarming consequences in terms of cybersecurity, as ISIS has already started building its own e-terrorism strategies not just for propaganda and recruiting purposes, but also for potential cyber-attacks in the future (Liang, 2017). Liang argues that ISIS is currently the most globalized terrorist organization in the world, that has increasingly been setting its sight on alternative methods of creating terror since its serious reduction in size and power recently (Liang, 2017).

In April of 2016, a group called the United Cyber Caliphate emerged, and is composed of many sub-divisions such as the Cyber Caliphate Army, Ghost Caliphate Section, Sons of the Caliphate Arms, and Kalashnikov E-Security (Liang, 2017). All of these groups belong to ISIS, and they are part of the terrorist group's new strategy and effort to wreak havoc on states. It is important to note that as of right now in 2019, none of these groups possess any sophisticated cyber skills, weapons, nor capacities. This does not mean however, that it will not change in the future and emerge as an increased threat to national cybersecurity, especially considering that ISIS still operates with millions of dollars (Liang, 2017). One does not necessarily have to be highly trained in cyber warfare when they can buy cyber weapons and toolkits in the Dark Web for bitcoin, and that is what is worrying.

CHAPTER FOUR

The Glass House

According to the U.S. Army's *Cyber Operations and Cyber Terrorism Handbook*, a cyber-attack is defined as a "premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives, or to intimidate any person in the furtherance of such objectives" (Faga, 2017, pg. 5). Under this definition, the United States has already been subjected to hundreds of thousands of cyber-attacks. The Handbook's definition was later expanded in 2016 to include the disruption of critical infrastructure, assets, and functions (Faga, 2017). This definition is a start in the process to begin criminalizing hostile cyber-attacks, but there is still much ambiguity regarding the concept of cyber warfare and how such attacks ought to be responded to.

American intelligence during the Cold War was developed to significant sophistication for its time, allowing U.S. intelligence to spy on the Soviets through their satellite transmissions, undersea telephone cables and other communication methods (Harris, 2014). Cyber technology never stopped evolving in the United States, but many scholars argue that it is evolving at a very slow pace and that this weakness is already causing damage to the U.S. One of the first major cyber security strategies adopted in the U.S. was in 2002, motivated by the 9/11 attacks which marked a new era for national security. This was when President George W. Bush signed the National Security Presidential Directive 16 which basically set out a plan for the development of national cyber weapons (Roberts, 2014). Furthermore, technologies were also developed to be able to infiltrate Iraqi insurgents through the internet and their communication methods, which allowed the U.S. military to track the insurgents down until they discovered why they kept getting caught.

Right after 9/11, the NSA, FBI, CIA, and DHS also began spying on U.S. citizens through the Patriot Act, in hopes of being able to find terrorist cells and prevent any further attacks within the United States (Harris, 2014). Advanced cyber operations need to be conducted by military personnel without the NSA because the NSA is not allowed to engage in war fighting or offensive responses to foreign attacks (Harris, 2014). Title 50 of the *United States Code* states that only military personnel are permitted to attack enemy systems and because of this, despite that many NSA staff are uniformed military personnel themselves, the Tailored Access Operations group (TAO) and other elite hacker groups do not have a very collaborative communication system with the other national security agencies (Harris, 2014). Thus, there is a disconnect between different sectors of national security within the U.S. and this disconnect may prove to be a huge obstacle in the future when cyber-attacks effectively take down SCADA and critical infrastructure systems.

In 2007, the office of the Secretary of Defense was attacked by Chinese hackers and it was forced to shut down and go completely offline in order to protect itself from further attacks and to be able to clean up its systems. Threats to our own democratic process and sovereignty one could argue, were first realized one year later in 2008 during the presidential race between McCain and Obama. During the race, the FBI discovered that both Russian and Chinese adversaries had infiltrated their campaigns and stolen huge amounts of information (Fuller, 2019). The fact that the same incident but on a much larger scale led to the same occurrence during the presidential race in 2016 is extremely alarming and is a clear sign that the "glass house" still remains largely unsecure.

In 2012, the Pentagon began building Plan X to create more cyber weapons like Stuxnet and come to "dominate" cyberspace (Segal, 2016). In conducting these attacks, however, the U.S. is launching attacks from within a glass house, as many scholars argue. The United States is currently a glass house because, although it does possess some of the most sophisticated cyber weapons in the world, its own defense systems are extremely weak and very easy for adversaries to infiltrate and wreak havoc. States are not the only adversaries that U.S. intelligence ought to worry about, as non-state actors such as ISIS have already attempted to infiltrate U.S. SCADA systems in the past. Though they failed, these events were simply a warning of the catastrophic events that could occur in the future if terrorist organizations do become capable of infiltrating critical infrastructures (Segal, 2016).

In 2013, President Obama signed Executive Order 13636 which called for the improvement of security in critical infrastructures an attempt to begin the process of patching up vulnerabilities that allowed adversaries to infiltrate these systems in the past (Kaplan, 2016). This was of imperative importance to President Obama, and despite efforts to securitize, in 2014 alone, there were almost 80,000 breaches of U.S. cyber security. What is even more concerning, is that the hackers involved in these attacks were able to remain undetected in the targeted networks for over 205 days until they were finally discovered (Kaplan, 2016). Govern and Finklestein argue that the United States has had many cyber security wake up calls, but that is has kept on pressing the snooze button and placed more attention on other issues both on the domestic and international level.

In 2016, President Obama proposed the Cyber National Security Action Plan (CNAP) which attempted to fortify collaboration between the private sector and the federal government regarding cyber security issues (Kumar, 2018). It also called for the allotment of a 35% increase in national spending on cyber security compared to the year prior and encouraged think tanks from both the private and public sector to engage and share information (Kumar, 2018).

The TAO

The Tailored Access Operations group is a team of elite hackers from the NSA who work both as “white hats” or, in other words, ethical computer hackers, and as cyber warriors to protect us. The number of TAO hackers compared to that of Chinese or Russian elite hacker groups is extremely small, there being only 300 people in TAO in 2013 compared to the thousands in adversary groups (Harris, 2014). Nevertheless, TAO has highly sophisticated technology and documents leaked by Edward Snowden a few years ago showed that TAO has implanted at least 85,000 spying devices in 85,000 computers in 89 countries around the world, and that this number is constantly increasing as TAO targets new enemy networks (Harris, 2014).

CYBERCOM

CYBERCOM was founded in 2009 and it is a cyber command group led by the NSA in

Fort Meade, Maryland. CYBERCOM coalesces national security networks systems with those of the Defense Department in order to provide strengthened cyber security (Brenner, 2011). This is one of the few ways in which private sector firms, the government, and the military come together and collaborate together to improve overall national security. Brenner argues that cross-departmental governance of this kind is exactly what is lacking in current cyber-security strategies in the U.S., and that this is one of the main reasons why our offensive capabilities are among the strongest, but our defense strategies are so weak (Brenner, 2011). In 2016, CYBERCOM had approximately 1,300 employees, again a very small number compared to adversary groups. Nevertheless, size does not equate with effectiveness nor capacity, and the United States currently has a highly sophisticated capacity which proved effective in the use of weapons such as Stuxnet.

Snowden's Betrayal

In 2013, Edward Snowden stole over 1.7 million confidential documents from the NSA while he was working there and released them to Wikileaks for the entire world to see. Wikileaks is an online outlet that reveals stolen classified information from governments around the world, and it was founded by Julian Assange in 2006. Brenner argues that due to Wikileaks and the fragility of cyber networks, secret information that used to be well protected now leaks through a fire hydrant and U.S. intelligence has not yet figured out how to make it stop. Nobody has, for that matter. Snowden announced the leak while he was in Hong Kong in 2013, and a few weeks later Wikileaks provided him with a plane ticket to Moscow and he has been hiding there ever since. The founder of Wikileaks, Julian

Assange also spent several years in hiding in the Ecuadorian embassy in London until April of 2019 when he was finally apprehended by British authorities.

Prior to Wikileaks, U.S. elite hacker groups had successfully infiltrated networks in South Korea, China, Iran, Russia, North Korea, Brazil, Germany, and many other states which were both adversaries and allies (Segal, 2016). After Wikileaks revealed that the U.S. was indeed spying on friend and foe alike, all of the targeted states took measures to protect themselves from further intrusions by U.S. intelligence. The leak of this information immediately caused diplomatic issues, especially concerning states like Brazil and Germany who are considered to be U.S. allies. Brazilian President Dilma Rousseff was set to meet with President Obama just days after Wikileaks released these reports, and in response Rousseff cancelled her visit to the White House. Wikileaks also revealed that the U.S. is not as well protected in the cyber realm as it made out to be, and this exposure put national security at very high risk up until this day.

One of the biggest national scandals caused as a result of Wikileaks was the discovery of NSA's PRISM program which was created in 2007 under President George W. Bush and expanded under Barack Obama during both of his terms. PRISM was basically an NSA partnership with all of the biggest brands in Silicon Valley such as Google, Apple, Facebook, Yahoo!, Microsoft and a few others (Levine, 2018). PRISM was an agreement between the NSA and these companies that allowed the NSA access to people's private accounts to gather information that may have been critical to national security (Levine, 2018). Whether this was ethical or legal is a subject for another debate, but the release of information on PRISM made Americans feel distrustful of and betrayed by the American government and in the process, PRISM also lost some of its leverage.

As often as 30 times a day, people send various top security documents to Wikileaks in hopes that they will get published on the official website and as there are no laws to prevent a PeRiQuito AB (PRQ) host provider website from operating, Wikileaks in a sense is considered legal. The PRQ internet service provider is a Swedish business, created in 2004, to give anyone on the internet a platform regardless of the activity taking place on that website. The criminals who leak and upload information to Wikileaks however, are subject to national criminal laws or potentially to whistle blower laws. Even if Wikileaks could be removed from the internet, it would take no time before similar websites appeared (Brenner, 2011). The U.S. Department of Justice has charged Snowden with violating the Espionage Act of 1917 and the theft of government property. Snowden's American passport was also revoked, and he has since been living in Russia as an asylee.

The Role of Congress

It is crucial that in the development of strategies to deal with cyber threats, the executive branch and Congress work together, as one cannot really do all that much without the other. There are some cases in which the executive may act alone in repelling an attack against the state, but at the same time Congress is also permitted to regulate those actions at all times unless the state is under attack (Dycus, 2010). Dycus argues that it is of imperative importance that Congress is successful in providing guidelines on how to deal with cyber-attacks, cybersecurity, and cyber warfare because if it does not, the executive may act on their own to try and solve these issues. This is certainly not the idea that the Framers had in mind, and in order to make significant progress and avoid such an instance, federal executive agencies and Congress must begin to work better together (Dycus, 2010).

According to [Executive Order No. 12,333], intelligence agencies such as the NSA, CIA, and the Defense Department, are to be "fully informed" about national efforts to deal with threats to the state, which includes cybersecurity related threats as well (Dycus, 2010). It is not clear nor specified however, what "fully informed" actually means and what it entails, which leaves much ambiguity in the discussion. The major problem with this executive order is that it does not guarantee that the Congress will receive any of that information given to intelligence agencies, which is crucial in the development of cyber warfare policy and strategy (Dycus, 2010). As has been argued previously, the disconnect between federal government agencies, the private sector, the Congress, is a major issue which has resulted in the lack of appropriate and necessary cybersecurity planning.

Dycus argues that the disconnect between all of these agencies and the military is even greater. There are instances when the military is not required to share secret information with Congress regarding operations, especially when they are dealing with "clandestine activities" (Dycus, 2010). Though the military activity may carry diplomatic, national, and international risks or consequences, secret military operations are allowed to remain secret until they have already been executed. Additionally, there are also cases where secret military operations, depending on their nature, are not required to be shared with either the President or intelligence agencies at all (Dycus, 2010). Even if this were not an issue, Congress still has not been able to arrange suitable guidelines for dealing with cyber warfare, and this is not just because of the disconnect between agencies but it is also because Congress has simply not prepared itself to adequately handle threats involving sophisticated attacks coming from computers (Dycus, 2010).

Dycus asserts that another reason why Congress has not been able to develop cybersecurity guidelines is because of the lack of domestic and international law dealing with cyber threats. Therefore, the development of a misinformed policy or strategy in cybersecurity could lead to violations of LOAC and other international agreements (Dycus, 2010). Nevertheless, the efforts of cooperation between Congress and the Executive have recently been evolving, particularly under the White House Cybersecurity Policy Review which recommends that the:

“Administration should partner appropriately with Congress to ensure that adequate law, policies, and resources are available to support the U.S. cybersecurity-related missions” (Dycus, 2010, pp. 167). This review came with a set of seventeen guidelines that set out the framework under which Congress and the Executive should work, tackling all of the problems mentioned above.

First, there must be one committee in each House that is responsible for creating legislation to deal with cyber warfare. Second, the designated committees must develop policies that can be implemented for offensive and defensive purposes regarding the use of cyber weapons. Third, these designated committees must oversee every government agency’s activities related to cybersecurity and cyber warfare, including military operations that are either covert, overt, or clandestine. This resolution aims to solve the disconnect between the military and government agencies that Dycus previously outlined, and that had been a major issue up until the creation of the White House Cybersecurity Policy Review. Fourth, a federal agency must be placed in charge of planning and coordination among agencies, placing Congress as the major point of the development of policy and communication (Dycus, 2010).

This resolution also aims at tackling the lack of communication between intelligence agencies and Congress, which had previously been a great obstacle in policy development. Fifth, there ought to be one leading agency that is responsible for the execution of the cybersecurity plan once it has been created and agreed on. Sixth, a declassified National Cybersecurity Strategy document must be produced in the most detailed fashion possible, with clear cut guidelines to inform Congress on how to proceed with the execution of the cybersecurity strategy. Seventh, briefings of the congressional committees must take place frequently in order to adequately ensure that guidelines, laws, and policies are being followed to guarantee a successful outcome. Eighth, there must be consultation with the congressional committees before any agency is to employ the use of cyber weapons in any space unless it is an emergency, and the President decides to employ the use of the weapons (Dycus, 2010).

Ninth, in addition to the approval of Congress to engage in the use of cyber weapons, there must also be a written agreement from the President stating that the executive believes that this sort of action is absolutely necessary for the national security of the state. Tenth, detailed reports of the use of those cyber weapons must be provided to government agencies so they may be informed. Eleventh, the withholding of information regarding such activity is absolutely forbidden, even if the information is deemed classified. Twelfth, it is required that all reports be properly delivered to all committees involved without exception. Thirteenth, offensive responses without consultation in dealing with cyber threats to the United States are forbidden, due to high chances of misinterpretation, anonymity and attribution issues that could occur and create serious diplomatic issues (Dycus, 2010).

Fourteenth, government structures must be created and designed in a way that adequately cooperates with the private sector when and if it is attacked, to ensure that they do not act or respond on their own without prior consultation. Fifteenth, existing legislation must be amended so that privacy within the United States is protected. This includes the patching of vulnerabilities within our networks, the monitoring of email related phishing attacks, and the designation of cybersecurity officers in charge of this monitoring process. Sixteenth, once the U.S. cyber warfare policy has been reached, it must be made available to the public to ensure maximum security efforts. Lastly, the outsourcing of operating cyber weapons must be prohibited without exception, whether it be for defensive or offensive purposes due to the consequences that could occur if they were employed erroneously (Dycus, 2010).

The White House Cybersecurity Policy Review is thus far the greatest effort that has been made in dealing with all of the issues of lack of communication and cooperation among government agencies, the private sector, and the military. It is also the best way to ensure transparency between agencies, so that cybersecurity efforts may be focused in a cooperative effort that ensures maximum strategic planning with possible higher rates of success. Nevertheless, the issue of ambiguity in international law will remain a major obstacle to such efforts on the international level, where a cyber "armed attack", cyber warfare, and cyber weapons have not yet been clearly defined.

CHAPTER FIVE

Strategies to Combat Cyber Threats Through International Law

Each author has presented a strategy in dealing with different aspects of security in regard to cybersecurity worldwide. Roberts and Dev place most attention on the importance of international law, as is the core argument of my thesis; Clarke offers an analysis on cyber deterrence following a similar model to that for the nuclear bomb, and Brenner focuses more on national security as a first priority, and possibly using sanctions as a form of deterrence to cyberwarfare. Each of these strategies are great for addressing different sets of issues or questions. Nevertheless, Roberts' and Dev's arguments regarding the importance of international law are the most important for this paper.

Shaun Roberts' Five Strategies

Shaun Roberts is an academic in cyber issues who offers five different strategies or approaches to combat the difficulties associated with the lack of applicable international law in cyberspace, and how to properly identify and classify each type of attack. The first of these is the instrument-based approach which looks at the nature of the cyber weapon itself and analyzes whether it has effectively disrupted state communication or not. If the attack has indeed disrupted state communication, Article 41 of the U.N. Charter could be applied as it states that:

“The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations” (U.N. Charter, art. 41).

Roberts argues that by using Article 41 in this approach, a cyber-attack cannot constitute an “armed attack” because it is not yet recognized on the same level of weaponry as a traditional weapon, but it can still constitute as an act of “armed force” (Roberts, 2014). Since the purpose of a large portion of cyber-attacks is to disrupt systems such as those outlined in Article 41 of the charter, it may be useful until there are more specific laws to encompass cyber conflict (Roberts, 2014).One of the major obstacles that I see with this approach however, is that the U.N. Charter does not apply to non-state actors and adversary states already know this, which is why they have been contracting non-governmental groups of hackers to conduct many of the cyber-attacks today. However, this could change if the United Nations Security Council decides that the Charter does indeed apply to non-state actors.

Second, the target-based approach looks at the specific target of the attack and where the attack was intended to cause the most damage. If the attack was aimed at damaging a state’s critical infrastructure, it may be regarded as an armed attack under the LOAC and other bodies of international law (Roberts, 2014). With this approach, however, the same issue of attribution still remains, and unless the attack can be attributed to a specific state, the target-based approach would be difficult.

Third, the effects-based approach focuses on the effects and aftermath of the cyber-attack itself. If the effects of the cyber-attack could prove to be as catastrophic or harmful as those created by a traditional weapon, it may be possible to treat it as an "armed attack" and apply the same existing laws to this scenario (Roberts, 2014). This sort of cyber-attack would have to cause civilian deaths and destruction of property, which could have been a possibility if Iran had succeeded in opening the sluice gate of the dam in New York in 2016. The fourth approach is the sovereign based approach which would equates cyber-attack to an armed attack if the attack interfered with a state's sovereign functions and rights (Roberts, 2014). In theory, one could argue that this event has already occurred in 2016 when the U.S. elections were interfered with by the Russians. Attribution of attack to a state will remain a problem even with this approach, and even if the attack were attributable there still remain bodies of international law and diplomatic relations which would impede a state from acting so quickly in response to an attack against their sovereignty.

The fifth and final approach is the non-kinetic effects approach, which emphasizes the violation of people's right to survival (Roberts, 2014). Under the U.N. Charter, non-kinetic attacks such as naval blockades can be treated as an "armed attack" because they directly impede the victims' right to survival via strangulation and economic punishment (Roberts, 2014). If the Charter could point to sufficient harm, a cyber-attack could be treated as an armed attack.

Priyanka R. Dev: The Expansion of the Tallinn Manual and LOAC

Dev is another scholar in the field, who argues that the most important component of cyber security is the development of international law because without it too many ambiguities in this new realm of warfare remain, making international relations very difficult. More specifically, states must come to a consensus on what constitutes a cyber armed attack, and what the use of force means when it is applied to cyber weapons (Dev, 2015). One of the proposed ways to do this is to expand the already existing loose definition of the use of force in Article 2(4) of the U.N. Charter, and make it include damage caused by cyber-attacks or cyber weapons (Dev, 2015). In addition, a new legal threshold for the use of force that fully encompasses hostile cyber activities and treats such attacks as a violation of state sovereignty, which is not currently included in Article 2(4).

Dev further notes that one of the main problems with existing law is that existing LOAC definitions of war only encompass kinetic, physical forms of damage, and while cyber-attacks could indeed lead to kinetic damage, laws regarding cyber security are extremely vague (Dev, 2015). There are seven different components that Dev argues are of particular importance in applying existing law. First, the severity of the attack is the most important thing (Dev, 2015). One must analyze how severe the attack is on both property and individuals. How much damage was caused to infrastructure or networks, for example, will be crucial in applying international law in accordance with the appropriate threshold that the attack can be attributed to (Dev, 2015). Individual damage is important for the same reason and may be of even more importance if individual damage leads to death of individuals, as this could arguably be regarded as an act of war.

The next important factor is immediacy, based on severity. This looks at how immediate action and response to the attack is needed in order to resolve the damage caused or to clear the system of malware, for example (Dev, 2015). Directedness then focuses on analyzing what was able to cause the attack in the first place, and what the overall consequence of that weakness created (Dev, 2015). After analyzing the entry point or points that the hackers used, securing ought to focus on how deeply the networks were infiltrated, in order to draw up a plan of action that would successfully eliminate all adversary access to those networks (Dev, 2015). This, Dev calls a strategy of “invasiness” measurement.

The more that an attack is measurable by any scale, the better that the attack can be classified as either being an act of force or not (Dev, 2015). This is, of course, only once laws have been properly enacted regarding what exactly constitutes as an armed attack or the use of force in cyberspace. This is a good strategy, but I think that it overestimates the capability of international law right now and in the near future as well. Even if an attack’s severity is measured and results in reaching the armed attack threshold by a cyber security agency, there are so many other institutions both governmental and non-governmental that would need to agree on whether the attack can really constitute as an armed attack or not. Measurability will remain irrelevant in cyber security strategies so long as national or international laws are not suited to deal with cyber-attacks.

After the process of measuring the attack has been completed, Dev argues that presumptive legitimacy or the analysis of law in accordance to the attack is necessary (Dev, 2015). In this process, one is to analyze whether the attack was unlawful, an armed attack, or if it was an act of the use of force (De, 2015). Again, international law will be a huge obstacle in this process and until this stops being an issue, we will only be able to get up to Dev's strategic point four of "invasiveness" (Dev, 2015). Similarly, Dev's last point deals with state responsibility in response to the attack being examined. Dev argues that the greater the attack and the greater the degree that the state is involved in conducting that attack, the more international instability it will create (Dev, 2015).

This is a great point; although the anonymous nature of attacks and issues of attributability will remain a major obstacle. However, if an attack were to be attributed to the wrong state in error, that in itself could cause greater international instability than the attack itself. Moreover, Dev's strategies are a great preparation plan for cyber security in the future but we are certainly not at the stage where most of these strategies can be exercised. Perhaps, we may never be either. Too many scholars and thinkers think about the future of cyber security and forget that the security of our networks and national cyber security is an issue that deserves immediate attention in the way that we are experiencing it right at this very moment. The United States has been deemed by various scholars as a glass house, and if this is true, security ought to be focused at the national level, and then, on the international level.

Richard Clarke: Cyber and Nuclear Deterrence

Clarke is an academic scholar who bases his argument on deterrence against cyber weapons by reverting to the way the nuclear weapon was handled when we found ourselves in a similar confusing situation. Nuclear deterrence was able to work because everyone understood how serious and dangerous a nuclear weapon was, especially after witnessing the attacks on Hiroshima and Nagasaki during World War Two (Clarke, 2010). As a result, however, cyber weapons have been regarded by many states as an alternative new way to attack their enemies because it is believed that cyber-attacks are a more efficient, clean, cost efficient and casualty-reducing form of attack.

One of the problems with trying to apply the nuclear deterrence model to cyber security is that with nuclear weapons, there is no real in-between. A state either launches an attack that will cause a lot of damage, or it will not use a nuclear weapon at all. In other words, nuclear attacks are extremely deadly and there is no way of launching a nuclear attack that would not be catastrophic for many reasons (Clarke, 2010). With cyber-attacks, there is a plethora of different ways one could attack and all with varying levels of severity. Additionally, with nuclear attacks there is no question about who launched the attack. With cyber weapons however, attributability remains a huge obstacle in being able to apply any form of deterrence at all (Clarke, 2010). Also, nobody really knows just how much damage a cyber-attack could really cause today. There are speculations, but there has not yet been a cyber equivalent to Hiroshima and Nagasaki, and therefore it would be difficult to convince states that cyber weapons may be just as dangerous as nuclear weapons, but for different reasons.

Clarke proposes that states should work toward not only developing international law in this new domain of warfare but also to limit the amount of cyber arms that one has, as was done with nuclear weapons (Clarke, 2010). The first problem with this is that for such a program to work, it would require honesty and transparency from all states, which may not be achieved so easily. Second, the nature of cyber weapons is very different from that of nuclear weapons, and at present, there is no real way to truly know how many cyber weapons one particular state has (Clarke, 2010). Third, states would have to sign such a treaty and ratify it in order for it to work, and this may not be of interest to many states. Another idea proposed by Clarke is that cyber weapons be classified in the same arena as biological and chemical weapons and therefore be banned outright (Clarke, 2010). It would also require state consent in order to be applicable.

Even if cyber weapons were to be limited to a certain number of arms per state or completely forbidden, non-state actors are the key in this issue. Russia and China have already employed non-governmental hacker groups to conduct attacks and to spy on the United States, and since those groups are not affiliated with the government, it would be extremely difficult if not impossible to legally prove that an attack or violation of any of these agreements came from a state. The cyber realm is accessible to absolutely everyone in this world who has a computer or a cell phone, and thus the possibility of millions, if not billions, of people learning the ability to use cyberspace for malice is unstoppable. All of these assumptions, including Clarke’s arguments are very hypothetical and that is precisely for the reasons that we do not yet have a legal playing field with cyber security, and ambiguities are much larger than any current ideas of deterrence.

Another major issue with adopting a deterrence model similar to that used with nuclear weapons, is that such an argument assumes that states are rational and that they all share the same strategic culture. Prior to the bombing of Hiroshima and Nagasaki, it was not well understood how severe the use of a bomb would be until it was already too late and the entire world witnessed the horrific events in Japan. This event caused a sense of horror that resulted in a dramatic impact on people's opinions regarding the use and possession of nuclear bombs. There has not yet been an achievement of horror with cyber weapons, and I suspect that until this event comes, cyber deterrence will be a very difficult task to accomplish, let alone being able to actually implement deterrence strategies in the aftermath, which again would require honesty and transparency from all parties.

Joel Brenner: A Sanctions-Like, National Security Approach

Brenner argues that the best way to handle cyber security given all of the current obstacles and difficulties is to focus security on a national level first. This includes trade regulation and contracting, which would ban companies from doing any kind of business with internet services that have been known to host botnets for example (Brenner, 2011). The government would put out a list of business and internet services that have previously engaged in cyber-criminal activity, and businesses would be forced to comply with the ban of companies on that list. It would still be difficult to attribute illegal activity to a specific source, but it is certainly a way to begin cracking down on cyber insecurity on the national level.

The second idea proposed by Brenner is to make service providers take more responsibility for securing their own networks and for keeping their customers informed at all times that there is a present threat, and especially when a botnet, malware, virus, or worm has infected any of their devices (Brenner, 2011). Internet providers already do this to a very superficial extent, but they mostly rely on other cyber security companies to do this job for them, and it seems that perhaps there is some sort of disconnect or lack of communication between the two. Internet providers and cyber security companies like McAfee and Norton for example, should team up and provide better services for their customers in a joint effort.

A third idea proposed by Brenner is to encourage the Federal Energy Regulatory Commission (FERC) to require the North American Electric Reliability Commission (NERC) to limit its ability of connecting to public networks, which have proven to be especially vulnerable (Brenner, 2011). This could cause conflict with anti-trust laws, however, and would need close analysis before practice. The more that utilities are connected to public networks, the easier it is for hackers to be able to get into those networks and wreak havoc. When Iran hacked the dam in New York, the system was immediately taken offline by national security who identified the threat before Iran could do anything with the dam. Taking it offline was the key in this issue, and perhaps taking more national systems offline may also help to deter threats for now. Cyber weapons which do not require online access to offline systems already exist, but it may at least help in deterring groups with less sophisticated cyber weapons.

Fourth, Brenner argues that attribution of attacks is highly important and that research to be able to identify attacks to their source ought to be of paramount importance to national security (Brenner, 2011). This strategy would be especially important if we already had existing law that governs cyberspace, including definitions of cyber armed attacks, cyber warfare, etc. But since we are not there yet, I do not think that placing so much time and effort on attribution is so important while our networks remain extremely vulnerable. The United States is currently a glass house in the cyber arena, and focus should be emphasized on strengthening it first.

The last major proposal made by Brenner, is to increase security regulations by making electric utilities disclose their risks and vulnerabilities in SCADA systems as well as their networks which are connected to the internet and public networks (Brenner, 2011). This information would only be available to national security agencies, and not to the public. Similar to the second proposed strategy, this method would encourage national security to work with critical infrastructure to identify and analyze threats to be able to provide a better response. Furthermore, attention would need to be focused on protecting what is critically important first, and then everything else. This is a great idea, so long as the disclosed information on SCADA systems' vulnerabilities can be ensured to not land in the wrong hands. The way in which this information would travel is extremely important and should be highly secure to make sure that those reports do not land on the internet at all and that they are not shared through email or any other means on a public network.

Brenner also holds the private sector accountable for our current vulnerabilities and argues that the private sector ought to collaborate more in eliminating cyber threats on the internet before they are able to reach host devices and launch attacks of any kind (Brenner, 2011).

This means that cyber security agents would have to monitor network systems all the time to search for malware, viruses, or worms that could potentially infect computers (Brenner, 2011). The private sector should also control who is on the system or network to begin with, and physical access to critical infrastructure should be strictly regulated (Brenner, 2011). Aside from these strategies, Brenner states that the private sector ought to patch up any loopholes in networks and to fix existing software vulnerabilities and this is because, according to the author, most cyber-attacks are received through those holes and therefore more attention should be focused on patching them up before adversaries get the chance to use them to infiltrate systems (Brenner, 2011). Furthermore, rather than there being specified elite groups of cyber specialists, everybody in the private sector should be educated on how to identify and treat threats to cyber security (Brenner, 2011).

The private sector and government officials should also be trained on how to behave abroad and which internet networks should be encouraged and forbidden from use depending on the country that the individual is in. Such guidelines should be set out by the Office of the National Counterintelligence Executive (Brenner, 2011). All of these ideas proposed by Brenner are much more attainable than those offered by Clarke and Roberts because these strategies focus on a national level, which is where most of our vulnerabilities currently lie. In focusing so much on making international law applicable to cyber security, we may be neglecting the glass house and making it even more vulnerable to attack at the same time. Focusing on national security first is a great strategy not only for our own protection, but also for competition with states who are doing exactly the same instead of focusing so much on the international level of cyber security.

The focus of national cybersecurity efforts now ought to be placed on securing the 2020 Presidential Elections, to make sure that a similar occurrence to that of the 2016 elections will not occur. Although we have witnessed the catastrophic outcomes that a hacked election can have, that does not make us any more prepared to handle the 2020 elections. This is because Fancy Bear and Cozy Bear have evolved to much greater capacity today and are much more sophisticated than when we encountered them in 2016. Additionally, there are new players that have come to the table recently that are also cause for concern. In the first week of October, Iran managed to hack Trump's re-election campaign, and North Korean hackers have also begun hacking government officials, and organizations that are working with the presidential candidates.

Russia has most certainly not left the game either, despite that it has not made news headlines yet. Russian hackers are undoubtedly preparing to target the 2020 elections, but the question is when, and who they will target this time. We have already witnessed the resurgence of Russian trolls on the internet spreading fake news and deep fakes through Facebook, and also the re-emergence of Cozy Bear and Fancy Bear with new capabilities. Iran's hacking of the Trump re-election campaign may be indicative that there is a shift occurring, but it is still too early to tell. Nevertheless, cybersecurity efforts to ensure that we are able to have a proper democratic election without foreign influence or intrusion must be of primary focus.

CONCLUSION

The future of international law and cyberspace remains extremely uncertain, primarily due to the first four reasons identified in the beginning of this essay.

1. Definition: There are currently no definitions on the national level that define cyberspace, cyber-attacks, cyber warfare, the threshold of an armed attack in cyber security, or how the use of force applies in cyber conflict that have been agreed on by national security agencies in the United States. Without these definitions, it makes it impossible to apply already existing law and even to expand it to fully encompass cyberspace related hostilities. There is a lot of disconnect between the private sector and the public sector regarding these definitions, and due to the lack of cooperation between these agencies, we have not yet arrived at a point where cyber-attacks from foreign adversaries can be responded to by law.

2. International Definition: It is already extremely difficult to come to an agreed upon definition on the national level, but it is equally as important to be able to achieve these definitions on the international level. This is because international bodies of law are best suited for states to perform in the international arena without severely causing instability and further conflict between states. There are bodies of law in the Geneva and Hague Conventions, as well as in the U.N. Charter, which could be expanded to include concepts of cyber conflict and therefore provide states with a plan of how to adequately respond to a cyber-attack. The law already exists and applies to kinetic conflict despite definitional issues, and it needs to expand further to consider cyber-attacks as either a new domain of warfare altogether or as armed attacks so long as they result in the destruction of property or the loss of life.

3. Anonymity in Cyber Attacks: Even if states were able to agree on a set of definitions and if law were expanded to encompass hostilities in cyberspace, there would still remain the issue of attribution. Cyber-attacks are anonymous in nature and although less sophisticated attacks are easier to attribute to the source, it is not always so easy to do so with highly sophisticated attacks coming from Russia and China for example. Malware is often used to infect hundreds or thousands of computers all around the world, which then unknowingly host a virus, which is then used by hackers to launch an attack emanating from all of the computers at once against their target. This makes it very difficult to identify the source of the attack and without being able to attribute an attack with certainty to a state, it is impossible to apply international law. The law deals on a state-to- state basis, and to further complicate things, Russia and China have begun using non-governmental hacker groups to conduct a vast amount of their cyber-attacks against the United States. International law regarding de facto organs of state however, can certainly be applicable in dealing with this issue.

4. Applying Existing Law: If all of these issues were to be resolved, the actual application of existing international bodies of law would still remain extremely difficult due to contradictory components of law. Article 51 of the U.N. Charter, for example, allows states to respond with the use of force in proportion to the attack of the adversary state. However, Article 2(4) of the United Charter bans the use of force against other states, which is also part of customary law. The Charter also fails to define what the use of force constitutes, nor what an armed attack really is. It vaguely addresses the issue, but not sufficiently. Therefore, contradicting law and lack of definition is a great obstacle for the use of the charter in cyberspace conflict.

The Achilles Heel

The Achilles heel of the United States is without a doubt the lack of national cyber security. This problem comes directly out of the absence of international law that deals with cybersecurity, which gives states no guidance on how to proceed when they are victims of a foreign led cyber-attack. The development of international law ought to be the very main focus of all states, if we are to adequately begin to address the cyber question. Though the U.S. has a strong military with highly sophisticated cyber weapons and technology, it is still in a very vulnerable position. Efforts of national security with regard to cyber security do not come anywhere near those of Russia and China, for example, which have taken great measures to protect their own infrastructures from adversary intrusion.

Therefore, the best approach to handling cyber security issues for the time being ought to be in protecting our infrastructure as much as possible, while building cyber weapons at the same time. The disconnect between the private and public sector is an issue that has halted national security efforts as there is a lack of communication and sense of direction between the two (Klimburg, 2017). If we are to improve our national security from future adversary threats, it is imperative that these sectors begin to work together more efficiently.

Joel Brenner proposes a list of ideas that could be used in focusing on national security efforts such as business regulation with offensive services, increase service providers' responsibility to the customer, the limitation of FERC and NERC to connect to public networks, and the development of attribution technology and strategy (Brenner, 2011). Brenner's work is significant to the focus of security in the United States in the realm of cybersecurity because it focuses on national security first, and international law as the next step. It is probably impossible to be able to protect all infrastructures, SCADA systems and networks in the U.S. as new technology weapons develop at a very rapid pace, but it is nevertheless imperative that more efforts be focused on the strengthening of networks.

Without attribution technology, as argued by Brenner in his fourth recommendation, it would be impossible to apply any sort of international law. International law only works on a state to state basis right now, and therefore in order to be able to apply any kind of law in response to an adversary attack, the victim state ought to know with certainty where the attack came from. If it is found that the attack came from a non-state actor, then law would be practically impossible to apply, but at least if the U.S. had the technology to attribute attacks to a state, it creates a legal playing field for states to respond accordingly. This conversation and effort ought not to be made alone, but rather the United States should be working with the European Union in these security efforts, because European Union states have been working on this sort of security for a very long time and they are perhaps some of the most secure states against cyber-attacks.

This joint security effort should focus on “confidence building and exchange of national views on the use of cyber information technologies in conflict, information exchange on national security strategies and technologies and best practices, further dialogue among countries, and finding possibilities to elaborate common terms and definitions” (Pool, 2013, pg. 24). Pool’s arguments focus on national security, but unlike Brenner, Pool argue that strong cyber security cannot be achieved alone and it ought to be done as a combined effort amongst allied states, particularly between the United States and the European Union. Richard Clarke further argues that the United States should also securitize itself by threatening to take kinetic action against states who attack through cyberspace. Even if the threat may not be serious, Clarke argues that the threat itself might be enough to deter states from conducting further attacks (Clarke, 2010).

Brenner and Clarke make very distinct arguments from Dev’s and Roberts’ propositions and while they all play a key role in the movement towards achieving some sort of global consensus with the new weapon, as was once reached with nuclear weapons, the role of international law nevertheless remains the most important aspect. Without it, states have no legal guidance on how to respond when they are attacked, and cyber weapons will continue to be developed by both states and non-state actors without any restraint or legal obligations to abide by. The absence of international law, along with the ambiguity of definition, will remain to be our greatest obstacles in cyber-insecurity into the future.

BIBLIOGRAPHY

Ackerman, Spencer. (2016). *The Plot to Hack America: How Putin's Cyberspies and Wikileaks Tried to Steal the 2016 Election.* New York, NY: Skyhorse Publishing.

Ayalew, Yohannes. Cyber Warfare: A New Hullabaloo Under International Humanitarian Law. *Beijing Law Review, 6, 209-223.*

Bagchi, A., & Bandyopadhyay, T. (2018). Role of Intelligence Inputs in Defending Against Cyber Warfare and Cyberterrorism. *Decision Analysis, 15*(3), pp. 174-193.

Baradaran, N., Homayoun, H. (2017). Cyber Warfare and Self Defense from the Perspective of International Law. *Journal of Politics and Law, Vol. 10, Issue 4, pp. 40-54.*

Barrett, E. (2015). Reliable Old Wineskins: The Applicability of the Just War Tradition to Military Cyber Operations. *Philosophy & Technology, 28*(3), pp.387-405.

Berger, M. (2017). The End of the War as We Know It: How an Act of Cyber Warfare Could Impact the U.S. Energy Grid. Journal of Technology Law & Policy, Vol. 22, Issue 1, pp. 141-164.

Bernstorff, J. (2009). Martens Clause. *Oxford Public International Law*.

Brenner, J. (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare.* New York, NY: Penguin Press.

Buchan, R. (2016). Cyber warfare and the status of anonymous under international humanitarian law. *Chinese Journal of International Law*, *15*(4), pp.741-772.

Carlin, J. (2018). *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Threat.* New York, NY: Hachette Book Group.

Carr, J. (2012). *Inside Cyber Warfare: Mapping the Cyber Underworld.* Sebastopol, CA: O'Reilly Media, Inc.

Cimbala, S. J. (2017). Nuclear Deterrence and Cyber Warfare: Coexistence or Competition? *Defense & Security Analysis, 33*(3), pp. 193-208.

Clarke, R. (2012). *Cyber War: The Next Threat to National Security and What to Do About It.* New York, NY: Harper Collins Books.

Crawford, J. (2019). Military and Paramilitary Activities In and Against Nicaragua Case (Nicaragua v United States of America). *Oxford Public International Law.*

Crespo, R. A. (2018). Currency Warfare and Cyber Warfare: The Emerging Currency Battlefield of the 21st Century. *Comparative Strategy*, *37*(3), pp. 235-250.

De Quadros, F., Stone, J. (2013). Act of State Doctrine. *Oxford Public International Law*.

Dev, P. R. (2015). "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, 50*(2), pp. 381.

Dycus, S. (2010). Congress' Role in Cyber Warfare. *Journal of National Security Law & Policy, Vol. 4, Issue 1, pp. 155-172.*

Engdahl, W. (2009). *Full Spectrum Dominance: Totalitarian Democracy in the New World Order.* Boxboro, MA: Third Millennium Press.

Faga, P. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. *Baltic Journal of* ***Law*** *& Politics, Vol 10, Issue 1, pp. 1-34.*

Fleck, D. (2013). Searching for International Rules Applicable to Cyber Warfare- A

Critical First Assessment of the New Tallin Manual. *Journal of Conflict and Security Law, Vol. 18, Issue 2, pp. 331-352.*

Fuller, C. J. (2019). The Roots of the United States' cyber (In)security. *Diplomatic History, 43*(1), pp. 157-185.

Gertz, B. (2017). *iWar: War and Peace in the Information Age.* New York, NY: Threshold Editions.

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York, NY: Henry Holt and Company, LLC.

Guiora, A. (2017). *Cybersecurity: Geopolitics, Law, and Policy.* New York, NY: Routledge.

Harris, S. (2014). *@War: The Rise of the Military-Internet Complex.* New York, NY: Mariner Books.

Harold, S., Libicki, M., and Cevallos, A. (2016). Getting to Yes with China in Cyberspace. Santa Monica, CA: Rand Corporation.

Harrison, R., Herr, T. (2016). *Cyber Insecurity: Navigating the Perils of the Next Information Age.* London, UK: Rowman & Littlefield.

Hayden, M. (2016). *Playing to the Edge: American Intelligence in the Age of Terror*. New York, NY: Penguin Press.

Ibor, A. E. (2017). Zero Day Exploits and National Readiness for Cyber Warfare. *Nigerian Journal of Technology, Vol. 36 Issue 4, pp. 1174-1183.*

Jajodia, S., Shakarian, P., Subrahmanian, V.S., Swarup, V., Wang, C. (2015). *Cyber Warfare: Building the Scientific Foundation.* Switzerland: Springer International Publishing.

Jamieson, K. (2018). *Cyber-War: How Russian Hackers and Trolls Helped Elect a President.* New York, NY: Oxford University Press.

Jordan, Thomas. (2016). The Law of Armed Conflict, Unconventional Warfare, and Cyber Attacks. National Security Law Brief, Vol. 6, Issue 2, pp. 37-58.

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War.* New York, NY: Simon & Schuster Paperbacks.

Kees, Alexander. (2011). Responsibility of States for Private Actors. *Oxford Public International Law.*

Kirsch, C. M. (2012). Science Fiction No More: Cyber Warfare and the United States. *Denver Journal of International Law and Policy, 40*(4), pp. 620.

Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace.* New York, NY: Penguin Press.

Kosseff, J. (2017). *Cybersecurity Law.* Hoboken, NJ: John Wiley & Sons, Inc.

Kovács, L. (2018). Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review, 23*(1), pp. 16-24.

Lewis, T. (2015). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Hoboken, NJ: John Wiley & Sons, Inc.

Levine, Y. (2018). *Surveillance Valley: The Secret Military History of the Internet.* New York, NY: Hachette Book Group.

Logan, K. (2018). *Homeland Security and Intelligence.* Santa Barbara, CA: Praeger.

Liang, C. (2017). Unveiling the "United Cyber Caliphate" and the Birth of the E-Terrorist. *Georgetown Journal of International Affairs, Volume 18, Number 3.*

Main, S. J. (2018). China's Cyber Warfare: the Evolution of Strategic Doctrine. *Europe-Asia Studies, 70*(9), pp. 1519-1521.

Mazanec, B., Thayer, B. (2015). *Deterring Cyber WarfareL: Bolstering Strategic Stability in Cyberspace.* New York, NY: Palgrave MacMillan.

Nance, M. (2016). *The Plot to Hack America: How Putin's Cyberspies and Wikileaks Tried to Steal the 2016 Election.* New York, NY: Skyhorse Publishing.

Nguyen, R. (2013). Navigating *Jus ad Bellum* in the Age of Cyber Warfare. *California Law Review, 101*(4), pp. 1079.

Palchetti, Paolo. (2017). De Facto Organs of a State. *Oxford Public International Law.*

Patrascu, P. (2018). The Appearance and Development of National Cyber Security Strategies. *ELearning & Software for Education, Vol. 4, pp. 53-59.*

Pehlivan, O. (2019). *Confronting Cyber Espionage Under International Law.* New York, NY: Routledge.

Piątkowski, M. (2017). The Definition of the Armed Conflict in the Conditions of Cyber Warfare. *Polish Political Science Yearbook, 46*(1), pp. 271-280.

Pool, P. (2013). War of the Cyber World: The Law of Cyber Warfare. *The International Lawyer, 47*(2), pp. 299-323.

Reveron, D. (2012). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Washington, DC: Georgetown University Press.

Raboin, B. (2011). Corresponding Evolution: International Law and the Emergence of Cyber Warfare. *Journal of the National Association of Administrative Law Judiciary, Vol. 31, Issue 2, pp. 602-668.*

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An Introduction to Cyber Peacekeeping. *Journal of Network and Computer Applications, 114, pp. 70-87.*

Rodden, J. (2015). Warfare, from Cold to Cyber. *Society, Vol. 52 Issue 5, pp.405.*

Russell, A. (2014). *Cyber Blockades.* Washington, DC: Georgetown University Press.

Salter, M. (2012). Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause. *Journal of Conflict & Security Law, Vol. 17 No. 3, 403-437* .

Sanger, D. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age.* New York, NY: Crown Publishing Group.

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York, NY: Hachette Book Group.

Schaap, A. J. (2009). Cyber Warfare Operations: Development and Use Under International Law. *Air Force Law Review, 64*, pp. 121.

Schmitt, M. (2017). *Tallinn Manual 2.o on the International Law Applicable to Cyber Operations.* Cambridge, United Kingdom: Cambridge University Press.

Schmitt, M. N., & Watts, S. (2015). The Decline of International Humanitarian Law *Opinio Juris* and the Law of Cyber Warfare. *Texas International Law Journal, 50*(2), pp. 189.

Shackleford, S. (2014). *Managing Cyber Attacks in International Law, Business, and Relations: In Search for Cyber Peace.* New York, NY: Cambridge University Press.

Simpkins, B., Bagett, R. (2018). *Homeland Security and Critical Infrastructure Protection.* Santa Barbara, CA: Praeger.

Singer, P.W., Friedman, A. (2014).*Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York, NY: Oxford University Press.

Springer, P. (2017). *Encyclopedia of Cyber Warfare.* Santa Barbara, CA: ABC-CLIO, LLC.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government Regulations in Cyber Security: Framework, Standards and Recommendations. *Future Generation Computer Systems*, *92*, pp. 178-188.

Stockburger, P. (2016). Known Unknowns: State Cyber Operations, Cyber Warfare, and the *Jus ad Bellum*. *American University International Law Review, Vol. 31, Issue 4, pp. 545-592.*

Turns, D. (2012). Cyber Warfare and the Notion of Direct Participation in Hostilities. Journal of Conflict and Security Law, Vol. 17, Issue 2, pp. 279-300.

Valeriano, B., Maness, R. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System.* New York, NY: Oxford University Press.

Warren, P., Streeter, M. (2012). *Cyber Crime & Warfare: All That Matters.* London, UK: Hodder & Stoughton.

Watts, C. (2018). *Messing With the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News.* New York, NY: HarperCollins Publishers.

Woltag, J. (2015). Cyber Warfare. *Oxford Public International Law.*

Zemanek, K. (2013). Armed Attack. *Oxford Public International Law.*