8-8-2019

The Future of War: Cyber-Attacks and Aggression in International Law

Jamie Hogan
Portland State University

The Future of War: Cyber-Attacks and Aggression in International Law

By

Jamie Hogan

An undergraduate honors thesis submitted in partial fulfillment of the

requirements for the degree of

Bachelor of Arts

in

University Honors

and Political Science: International Development

Thesis Advisor

David Kinsella (Ph.D.)

Portland State University

2019

Introduction

Over the last fifty years, technology has been developing at a rapid rate. As this technology has developed, so has the threat of this technology being used as a weapon of war. Cyber threats are becoming increasingly visible; data breaches, social media propaganda, and ransomware attacks are happening all across the world. But can these threats become so grave that they could spark a war between states? An act of war typically constitutes an act of a conventional use of force, such as a bombardment, or invasion by one state against another (UN Resolution 3314), but as technology advances can a war be started with a few lines of code? This line of thinking is a new one to the international community, as thirty years ago these threats did not exist. As this threat continues to rise and pose a threat to the international community, the question must be addressed, can a cyber-attack rise to the level of being considered an act of war?

The attack itself is not the only area of concern when it comes to cyber-attacks, as with any new innovation, the long-term effects are unknown. There may be unintended consequences, and other areas of concerns with these types of attacks. This technology is in its infancy, and because of this, there are no international laws regulating the use of attacks. This lack of regulation, or even discussion about cyber-attacks, puts the international community at risk, because it means there are no constraints on when and how these weapons are deployed, and there is no way for states to seek redress for the damage inflicted by these attacks.

My research aims to determine what type of cyber-attacks could constitute an act of war, the conditions that would have to exist for a cyber-attack to be considered an act of war, and looks at the international community's response to this rising threat. I argue that cyber-

attacks can be considered acts of wars. They should be looked at through the same framework as any conventional attack in international law. In order for a cyber-attack to rise to the level of an act of war, the attack must; cause enough physical damage that it is akin to a conventional attack and the attack must be attributable to an actor. If these two conditions are met, then a state may invoke their right of self-defense and respond to the attack just like any conventional act of war, with a proportional response that can be either cyber or conventional in nature.

Methods

For my research, I will be conducting a literature review. This review will mostly be focused at the existing discourse in just war theory. Just war theory has been in existence for thousands of years, and addresses when actions before, during, and after the conclusion of wars, are just. It is built around a moral and customary law framework that has continued to evolve throughout history. I will specifically be looking at whether a cyber-attack can be considered an act of aggression, which will place my work within the framework of jus ad bellum, or the resort to war. The framework presented in just war theory has been codified into international law through the UN Charter, as well as in subsequent treaties such as the Geneva Conventions. I will specifically be addressing the just cause criteria of jus ad bellum, not making any conclusions about whether states should engage in wars that involve cyber-attacks, but observing the criteria it would require for cyber-attacks to fit the question of just cause (Dipert 2010). And I will be address proportionality of responses states could take if they enter into a war in response to a cyber-attack.

Just war theory is the foundation of international law regarding states engaging in war. In the last eighty years, treaties such as the UN Charter, and Geneva conventions were treaties that were codifying the customs of just war theory into international law. As part of my research I looked at the laws surrounding jus ad bellum and how the idea of cyber-attacks could fit within this existing framework. I also looked at rulings from the International Court of Justice, that have attempted to clarify areas of the law after an international incident occurred.

Finally, I looked at the scholarship that already exists about the use of cyber-attacks. Most notably I looked at scholars who have studied the worm known as Stuxnet, the most well-known cyber-attack, and the only one that could fit within the definition of a cyber-attack I will discuss in the next section. By examining these authors and their interpretations of the weapon, and more specifically the response to it, can the world begin to understand the threat of cyber-attacks through the damage that has already been inflicted.

What is a Cyber-Attack

In order to discuss cyber-attacks as a weapon of war, the first question that must be addressed is, what is a cyber-attack? The best way to think of a cyber-attack is by thinking of a cyber-attack as the means of carrying out an attack, not the target of an attack. Cyber-attacks are just a new form of weapon, just because cyber is in the name does not change the way of thinking about the weapon. Just as the way that an airstrike is an attack from an aircraft, and not an attack against an aircraft, a cyber-attack is weapon from a computer. (Nguyen 2013). The computer is just how the weapon is launched. This framework helps to understand how a cyber-attack can cause physical damage to systems that are not networks or computers.

The definition of cyber-attacks that will be used in this paper is: a *hostile act using computer or related networks or systems to cause destruction for a political or national security objective* (Nguyen 2013). It is important to note this definition is one of scholarly development and does not carry any weight of international law. There are other forms of cyber threats that can, and have been deployed throughout the world, not all of these actions line up with the definition used here, and thus they will not be the focus of this work.

Cyber-threats come in a variety of different forms. The most common way to think about a cyber-threat is through the lens of theft, or information warfare. The idea that an actor can "hack" into a system and steal valuable data or information. From an international law standpoint, these types of attacks are essentially espionage, which is neither condoned or condemned by the international community (Nguyen 2013). Although the espionage may have occurred via a network, the overall implication is that information has been stolen. Whether the theft of information was achieved through an actor getting into a system and stealing a file, or a foreign agent getting into a facility and stealing a file, ultimately doesn't make a significant difference. That is why this form of attack, information warfare, will not be discussed in this paper. It does not fit within the definition used above which includes the criteria of the attack causing physical damage. While this is an area of concern, espionage and other forms of information warfare are not new in the international system.

There are also questions surrounding Russian interference in the United States' 2016 election. These acts should also be considered acts of information warfare, through the use of propaganda, and disinformation, these tactics alone did not cause physical damage to the United States. The violation of the United States sovereignty is something that should be

addressed in international law, but this form of a cyber threat will not what will be addressed in this paper.

Another form of cyber-attack that has happened in recent history are the attacks in Georgia and Estonia. These are referred to as a disruption of service attack. In these cases, foreign actors were able to overload government systems and websites by increasing the number of systems attempting to use the site, and causing them to crash. Essentially it was like a ticketing website going down after tickets to the Super Bowl are released; so many people are trying to access the website, it gets overwhelmed and crashes. In the case of Estonia in 2007, the attackers targeted the banking infrastructure of the country. This caused a chain reaction as people, industries, and governmental departments were unable to access their money (Eberle 2013). Although this form of an attack did cause some disruption to the country, no one was killed, and there was no direct physical damage caused by the attack. There may have been damage sustained, however the damage was caused by actions that were steps removed from the cyber-attack, not a direct result of the attack itself. Disruptions of service attacks can cause significant impact on governments and industries, but they themselves do not cause physical damage, and also will not be the type of attacks discussed in this paper.

Physical Damage

It is important to address of the main points of the definition of a cyber-attack used in this paper, and its implication within the discussion around legal framework of war. War is a physical action, it causes death and destruction. When a conventional attack is launched, there is something left behind, whether it is causalities or damage done to a structure or area. This is

why the definition of cyber-attacks used in this paper looks to meet this same standard. A cyber-attack must create physical damage, so that it can though of in the same framework as a conventional act of war.

This physical attack also must be part a direct result of the attack itself, not degrees removed. For example, a cyber-attack could consist of increasing the speed of a train, so when it goes into a turn, it derails. The derailment would be a direct result of the cyber-attack. However, if a cyber-attack were to cause the train to come to a sudden stop, causing the cargo to come loose and hit someone in the head, this would be a degree removed from the cyber-attack. The attack itself was not launched with the intention to cause the cargo to go flying, it just happened to be a consequence of the attack. Its direct objective in this case was to cause the train to stop. This distinction is very crucial to understanding cyber-attacks. Otherwise almost any form of information warfare could be considered a cyber-attack as well.

Information warfare is taking place all around the world, just this year, a ransomware attack was launched against the city of Baltimore (Chokshi 2019). The city government had been locked out of their systems, and the only way to restore their access was by paying the perpetrators. Over the last few years, numerous companies have been breached, actors have been able to access credit card information of those who shopped at places such Home Depot or Target. These attacks are why it including the criteria of physical damage in the definition of cyber-attacks is so critical. The information warfare attacks are criminal in nature, even though they are using cyber technology, they essentially are acts of blackmail and theft. Cyber-attacks are attacks that use the same means, but far more drastic ends. Cyber-attacks cause destruction which could rise to the level of being acts of aggression.

If a cyber-attack can cause enough physical damage that on its face it resembles an airstrike, or a bombardment, or any other conventional attack that would meet the definition of aggression, it too is an act of aggression. Aggression is about the result, not the means of achieving the result.

Stuxnet

As far as the world knows, there is only one documented attack that would fit the definition of a cyber-attack discussed in this paper. This attack, a worm dubbed Stuxnet, was discovered in June 2010, and was found to have infected over 60,000 computers worldwide (Farwell and Rohozinski 2011). Stuxnet was a worm, meaning that it did not require any additional direction from a human operator after it was initially released, and did not require the operator of the targeted device to activate. It would progress from system to system without any intervention, and without the operator of the system becoming aware that it is there (Farwell and Rohozinski 2011). The worm was unlike anything the world had ever seen, and once it was discovered, it was traced back to its initial target, an Iranian nuclear facility in Natanz. What made this worm so interesting was the way in which it operated and the damage it caused (Farwell and Rohozinski 2011).

The worm was discovered on roughly 60,000 computers, but it didn't do anything to these systems. The worm was set to only activate under very specific parameters, in this case a Siemens operations controller that used Windows. Essentially the worm would get into a system, check to see if the system met these parameters, and if it didn't find them it didn't match its target, it would move on. This of itself was an incredibly new and sophisticated

technology, no one had seen a worm that was able to distinguish between targets like this before. Only when it found a system that met its conditions then it would activate (Langner 2011).

The worm was designed to cause damage to the centrifuges that enriched uranium. The Siemens controller it was targeting controlled these centrifuges. Once the worm got in, it would adjust the speed of the motor of the centrifuges, intermittingly slowing them down and speeding them up to rates that were detrimental to the motor. Over the course of a few months in these detrimental conditions, motors on the centrifuges would fail (Farwell and Rohozinski 2011). Because Natanz was a classified facility, official data hasn't been released about the damage that it incurred or the number of centrifuges damaged, but in a report by 60 Minutes, Liam O Murchu discusses how roughly one to two thousand centrifuges were removed from the facility at Natanz during the time that Stuxnet was in operation (60 minutes. Stuxnet 2012). Or as Nguyen put it, the worm caused physical damage to centrifuges akin to the level of damage that could have been caused by an airstrike (Nguyen 2013).

While this was happening, the individuals running the facility had no knowledge that anything was amiss, because in another demonstration of how advanced this worm was, once it began adjusting the speed of the centrifuge, it would also change the control display, showing the operators that nothing was wrong with the systems. As Ralph Langner, one of the first people to analyze Stuxnet, said, "It's just like in a Hollywood movie, where the bad guys feed observation cameras with unsuspicious prerecorded input. In the same manner, Stuxnet replayed prerecorded input to the legitimate code during the attack" (Langner 2011). This meant that the Iranian officials who were operating the facility thought that their equipment

was operating normally, leaving these operators no course of action in addressing the problems they were facing, since according to their displays, there was not a problem.

Although this attack was unleashed a decade ago, it is still uncertain about who developed and launched this attack against the facility in Natanz. While the international community widely believes that the attack was orchestrated by The United States and Israel, neither country has claimed responsibility over the attack.

Stuxnet will serve as the main example of a cyber-attack throughout this paper, as it fits the definition of a cyber-attack, and points towards the future of war. Stuxnet was a worm that was able to cause immeasurable damage to the Iranian nuclear program, a national security objective for Iran. Not only did it cause the destruction of these centrifuges, it halted Iran's enrichment of uranium and resulted in years of delays in Iran's nuclear development (Nguyen 2013). Had this attacked happened through convention methods of war, Iran would have had the right to invoke their right of self-defense and respond to this attack.

Aggression

War has been one of the few constant occurrences throughout history. One thing that has changed about wars however, are the reasons for which they have been fought. For thousands of years, wars had to do with resources or spreading ones' influence on other cultures, or as Aristotle described it, wars are about acquisition (Kinsella and Carr 2007). In today's world, there is only one legitimate reason for states to go to war, self-defense.

According to article 51 of the UN Charter, states may invoke the right of self-defense after an armed attack has taken place against them. This begs the question, what constitutes an

armed attack? The International Court of Justice made a ruling on question in the case of *Nicaragua v. The United States*. In their decision the court ruled that there are two different uses of force in international conflicts; those that are the "most grave forms of the use of force" and "other less grave forms". These most grave forms are armed attacks, while the less grave forms have come to be referred to as frontier incidents. Only armed attacks warrant a states' right to invoke self-defense (Yusuf 2012). The challenge has been determining the line between these two different uses of force. This question has sparked much debate, and the concept of cyber-attacks adds to the confusion. Can these attacks ever rise to the level of being egregious or grave enough to fit the definition of an armed attack?

Yes, they can. Cyber-attacks are just the means by which an attack occurs. The concept of an armed attack does not distinguish between the weapons that were used, just the end result. Article 51 states "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations". If a member state perceives the act rises to the level of being egregious enough to be considered an armed attack, they may invoke their right of self-defense. But this still does not answer the question of where the line is between these two uses of force.

A perhaps more concrete way to look at this line is by looking at aggression. Article 39 of the UN charter discusses acts of aggression, stating that the security council will address acts of aggression. However, no definition of aggression is given in the Charter. In 1974, the UN looked to address this concern by passing Resolution 3314. This resolution gives two definitions of aggression, the first being that some acts of aggression are prima facie or acts that on its face are acts of aggression. Simply, aggression is the first use of force in a conflict, and this can be

determined by comparing the actions to other acts that have taken place throughout history. Some attacks are of such magnitude that they are easy to determine on their face that they were an act of aggression. The other definition the resolution provides is a non-exhaustive list of actions that may constitute an act of aggression, such as acts of invasion, bombardment, or a blockade (Resolution 3314), this provides a more materialistic definition of aggression than the prima facie definition that provides a place for interpretation.

Since the definition of aggression was passed by the UN in 1974, the UN did not list cyber-attacks as a form of aggression. It does not fit the first definition as there are no historical cyber-attacks in which to compare any attack today to, and thus no way to recognize an attack on its face as an act of aggression. And while the second part of the definition of aggression explicitly states that the list of acts is not exhaustive, they are all examples of conventional attacks. In order to discuss a cyber-attack in the existing framework of aggression, cyber-attacks then must be equated to physical attacks to understand their impact.

As stated before, the damage Stuxnet inflicted could be equated to the damage an airstrike would inflict (Clarke 2010). Equating a cyber-attack to conventional attack is the only way in which to address the questions of how these attacks fit into existing international law. Through this juxtaposition, and the fact that the second definition of aggression is a non-exhaustive list of acts, means that cyber-attacks fit can fit this definition. They can constitute acts of aggression, as long as they are comparable to conventional attacks.

As cyber-attacks become increasingly less rare, they may also fall into the first definition of aggression. The first definition was designed to open the definition up to interpretation. Now that Stuxnet has been discovered, if a similar attack were to occur, a state could make the

argument to compare the attack to Stuxnet to determine if this new attack is a prima facie act of aggression.

Attribution

After determining that an act of aggression was committed against a state, the next step is determining who launched the attack. However, this is not as straightforward as it is with conventional attacks. The so called 'attribution problem' is one of the greatest concerns regarding cyber-attacks (Nguyen 2013). As stated above the only legal reason to go to war in today's society is through invoking the right of self-defense, but the right is useless if you do not know who to respond to. In conventional warfare, determining the identity of the attacker is not challenging (Dipert 2010). The Geneva Conventions outline rules of engagement regarding how combatants must identify themselves, and prohibits states from engaging in false flag operations. These treaties were put in place to protect civilians, and to allow combatants to identify one another (Geneva Convention relative to the Protection of Civilian Persons in Time of War, 1977). With a cyber-attack this is not as simple. Cyber-attacks do not come with an insignia declaring who launched the attack. They may even attempt to conceal where they were created.

Although it well accepted in the international community that the United States and Israel were behind Stuxnet, neither state has ever claimed responsibility, and as far as we know, Iran has never responded in kind to the attack. Levi Grosswald details a reality that society may face as the use of cyber-attacks increase, and the damage that could ensue if a state is unable

to determine the aggressor state, or makes a determination about who the aggressor state is without being able to verify it.

> "…Day 12: A factory in Detroit blows up, destroying the eastern half of the city. After reviewing circumstantial evidence, the military suspects Russia and China are the masterminds. Both countries deny any involvement. Day 20: The United States retaliates physically while covert cyberattacks shut down both Russian and Chinese power grids. Oil pipelines in both countries are disrupted. Transportation, financial and power systems are shut down, causing immeasurable economic damage. Reports indicate that the number of Russian and Chinese deaths far outnumber those suffered in the United States. Day 25: After the attacks subside, U.S. Information Warfare Command obtains user identification data… The data is traced back to civilian-led liberation groups in the Republic of Abkhazia. Attackers merely routed strikes through Russian and Chinese networks…"(Grosswald 2011, 1151)

This terrifying excerpt explains the damage and destruction the world could incur if a cyber-attack was deployed, and was designed in a way to conceal who launched it. Deception like this could cause catastrophic damage as actors attempt to determine who attacked them, and in the midst of this chaos, jumped to conclusions. Attributing an attack to a state is to hold that state responsible for the damage. If states are unable to hold each other accountable for acts of war, with or without deception, then there is no way to stop these attacks from occurring.

States fear the repercussions of their actions, but if their actions could not be attributed to them, they could operate more freely. If North Korea for example, could launch a cyber-attack that stopped the thrusters on a U.S. surveillance satellite, causing the satellite to fall out of orbit, and be able to do so without the United States knowing that is was them, there would

be no deterrent to stop them. There would be no fear of retaliation through sanctions or through a conventional attack. They could simply get away with it, and if the U.S. could not determine who was behind the attack, then they could not do anything about it. North Korea could continue the same operation over and over again, against the United States, or against any other state they consider an enemy.

There is also the question of non-state actors launching cyber-attacks. In the disruption of service attacks against Estonia and Georgia, it is believed that Russia was behind the attacks, however, Russia claims that it was a non-state actor that just happened to reside within Russia's territory (Eberle 2013). According to the International Court of Justice in the case *Nicaragua v. US* (2003), states can only be held responsible for actions of non-state actors if they are exercising "effective control" over a group. In the case of the Estonian and Georgian attacks, the only way to hold Russia accountable would be to find evidence of the Russian government giving these groups direct orders to carry out these attacks. In the future, a cyber-attack that causes physical damage will be put against this same standard.

Being able to attribute an attack is absolutely vital to international society. Since there is no supranational entity, states have to hold each other accountable. If states are able to disobey international law the entire system falls apart. If sates cannot hold each other accountable, then they cannot seek redress for actions committed against them (Grosswald 2011). That is why if a cyber-attack is to be considered an act or war, states have to know who launched it. Without this information, there will only be more damage done.

Response

As stated above, once an armed attack has occurred, the victim state has the right to respond to the attack by invoke their right of self-defense. The one constraint of this response is the principle of proportionality. The victim state needs to respond to the initial attack in a way that is proportional. This principle is meant to prevent further escalation of the conflict.

This principle of proportionality, is not proportionality of means, it is proportionality of ends. If a state is the victim of a cyber-attack, this does not mean that they are required to respond in the same manner. They do not need to respond to the cyber-attack with a cyber-attack. They are allowed to respond to the attack with whatever means they deem fit. In the case of Stuxnet, if Iran had decided to invoke its right of self-defense, it could have responded to the attack with an airstrike that would have done a similar amount of damage as the worm did to its facility.

This principle may be a challenging one to meet. In regards to cyber-attacks, there is still so much that is unknown about their potential use and their potential threat. The Stuxnet worm went beyond its original goal, infecting more computers than intended. This could happen again, after a proportional attack is launched, it could accidently surpass this proportionality, because of the unknowns of cyber-attacks.

This response also brings back the attribution problem. States have to be able to determined who launched the attack in order to respond. As was discussed is the exert from Grosswold from above, states may misidentify who launched the attack. If the aggressor state is misidentified, the so called response could be act of aggression, and not proportional in its response at all.

Unintended Consequences

The world had never seen the likes of Stuxnet when it first appeared. Actors did not know how the worm would behave. The initial target of the worm was an air gapped facility, meaning that the facility was not connected to the internet. This set-up was supposed to serve as a safeguard for the facility, to protect it from cyber-attacks. Because of this set up, the worm must have been brought in to the facility on something like a flash drive (Farwell and Rohozinski 2011). While this was an obstacle that the states who deployed the weapon would have been challenged with, in the end this set-up also served as a containment system. Once the worm was released it should have stayed contained at the Natanz facility. This however was not the case.

The reason the world found out about Stuxnet is because it was unleashed on the world. It is believed that the worm was on an engineer's laptop that was removed from the site and then connected to the internet. Unlike conventional attacks, cyber-attacks are not limited geographically, and once it was released from the air gapped system, the worm spread. (Nguyen 2013). As discussed above, the worm was so sophisticated, it would only attack systems that met very specific parameters, but its mission was also to keep spreading until it found these conditions (Farwell and Rohozinski 2011). The worm exploited a weakness in the in the Windows operating software, meaning any computer running Windows was at risk to the worm; that was until Microsoft was able to create a patch to stop the worm (Langner 2011). But this did not happen until after the worm had managed to infect over 60,000 computers, and had found its way on to an Indian satellite (Farwell and Rohozinski 2011). Since these systems did not meet the criteria that Stuxnet was looking for, no damage was done to these

systems, however if the worm had not been as well designed as it was, it could have inflicted damage to thousands of computers (Nguyen 2013).

The world has seen what can happen if a cyber-weapon is coded incorrectly. In the early 2000s, Robert T. Morris designed a worm to determine how large the internet was. However he made an error when developing the code and launched a disruption of service attack on the entire internet (Nguyen 2013). Since worms such as Morris's and Stuxnet operate without human intervention, they are unpredictable. Once released they can spread to any system, and even if they are not initially designed to cause harm, the code could be corrupted during the transfer from one device to another, thus causing harm that was never intended. In Morris's case, he was a man attempting to learn something, not to cause any harm, but if this type of error, or a coding issue were to take place with an actual cyber-attack, it is unknown what kind of damage it could inflict.

This is not the only problem with cyber-attacks, they are just like any other weapon, prone to evolution and advancement. Another concern about cyber-attacks is what happens after they are discovered, the fact that by deploying them, states are actually inflicting harm on themselves in two ways. First it shows other states what they are capable of, showing how advanced their cyber-weapons have become. This allows the enemy to know what the state is capable of, and allows them to address this threat and prepare a way to neutralize it. Second, by releasing the weapon, states are essentially arming their enemies with a way to attack them (Clarke 2010).

With any traditional weapon once they are used, they are destroyed. After a bullet has been fired, it cannot be fired again, and certainly cannot be picked up and immediately

reloaded into the enemy's gun. With a cyber-attack, once it has been unleased, not only can it be used again, it can be turned back on the actor that used it first. In 2017, it was discovered that the NSA had found a weakness in Microsoft's Windows operating system, specifically a system that allows Windows machines to communicate with each other. Once they discovered this weakness, they developed a code that would exploit it. This system was called EternalBlue. A group called the Shadow Brokers released the information about the NSA's system, and within just a few months of this release, two different ransomware attacks were launched. The first one, WannaCry was developed by North Korea, and the second Petya (and an updated version NotPetya), both utilized EternalBlue. Although Microsoft was able to develop a patch to prevent this weakness from being exploited, EternalBlue has been used as a foundational element of malware attacks since then. Systems that are older, or air gapped may not have received the patch, and thus are still vulnerable to EternalBlue (Newman 2018).

After Stuxnet was discovered within months its technology was well known (Farwell and Rohozinski 2011). With how quickly the legacy of EternalBlue has been painted by scandal and exploitation, it is not a stretch to believe that states have learned a lot from Stuxnet and the way it operated. Stuxnet's technology most likely has been used to launch cyber-attacks somewhere in the world since its release. Armed with the information of how the worm was discovered, those involved may have been able to cover their tracks more effectively, which is why the public does not know about other cyber-attacks.

Looking Ahead

The world of cyber-attacks will only continue to grow as weapons become more and more advanced. These weapons are still relatively new, and essentially in their infancy (Nguyen 2013). Currently, there is nothing in international law to address these new weapons. The only discussions around cyber-attacks in the international community have revolved around lex lata, or existing law, as was examined in this paper. There have been no discussions surrounding lex ferenada, or future law (Schmitt 2014). Just as arms control treaties were created following the creation of nuclear weapons, treaties need to be created addressing the threat of cyber-attacks. They are a new form of weapon that, unlike nuclear weapons, every state could develop and deploy against one another. The question around these cyber-arms control treaties would then become how to enforce them (Dipert 2010). If every state and many non-state actors had the capacity to develop these weapons, there would be no way to regulate them.

The best way, and yet one of the most unlikely ways to address the threat of cyber-attacks is to solve the attribution problem (Dipert 2010). If states remove the element of anonymity, states would fear the consequences of their actions just as they would any conventional act of war. It would be impossible to require states to somehow "flag" their attacks to identify themselves to their enemy, and even if there was international law that would seek at address this concern, if a state violated this, there would still be no repercussions, for they would be unidentifiable.

One step that the International community could take would be to actually define what constitutes a cyber-attack. Establishing a definition so that the world could recognize the impact these attacks have would be a first step. This definition may be similar to the one used

here, addressing only actions that cause physical damage to defined as cyber-attacks, or perhaps expanding this definition in order to include actions such as disruption of service attacks. Only once this area has been more clearly defined can the international community begin to take steps to address it. Beginning with acknowledging that actions like those of Stuxnet, do fit the definition of aggression, and can be recognized as a legitimate act to trigger the right of self-defense if they can be attributed. This would lay the groundwork for continuing the discourse over the regulation of cyber-attacks.

After the fallout from Stuxnet, the Obama administration restricted the use of offensive cyber-attacks without the President's explicit approval (Clarke and Knake 2019). In President Trump's 2018 National Security Strategy, he outlines the threat of cyber weapons, and discusses defensive actions that need to be taken to keep the United States safe from cyber-attacks (NSS 2018). However, it has also been reported that President Trump removed the restrictions for offensive capabilities that President Obama put in place (Clarke and Knake 2019).

Conclusion

Attacks like the Stuxnet worm show that states are changing how they engage in conflict with one another. Just as with any other transitional moment in the development of weapons, the world is unaware what the next step may be. But as history has shown, wars will always be a part of life in the international community.

Cyber-attacks can rise to meet the definition of aggression. They are weapons just as any other conventional acts, that can cause physical damage and destruction. This needs to be

established so that when a cyber-attack is launched against a state, they have the right to defend and protect themselves by invoking their right of self-defense and responding in a proportional manner, which could be in the form of a cyber-attack, but does not have to be.

There is no international law regulating the use of cyber-attacks. These weapons are still in their infancy, and are only going to become more sophisticated and dangerous as technology advances. States need begin to address this threat now, in a proactive manner, rather than in a reactive manner that may result in more destruction. States need to react as they have done in response to threats in the past. Negotiate treaties, first outlining the definition of a cyber-attacks in order for states to know and understand the threat they are facing. From there, states need to discuss rules and regulations in regards to the use of these weapons, attempting to answer questions such as the attribution problem.

Stuxnet was launched a decade ago, meaning that more threats of this nature are either in development, or have already been deployed. Cyber-attacks are not just the future of warfare, but also the present, and the international community has an obligation to protect themselves and each other from this growing threat.

Bibliography

"60 Minutes. Stuxnet." 2012.

"070-19841126-JUD-01-00-EN.Pdf." https://www.icj-cij.org/files/case-related/70/070-19841126-JUD-01-00-EN.pdf (July 16, 2019).

Arquilla, John. 1999. "Can Information Warfare Ever Be Just?" *Ethics and Information Technology* 1(3): 203–12.

———. 2011. "The Computer Mouse That Roared: Cyberwar in the Twenty-First Century." *Brown Journal of World Affairs* 18(1): 39–48.

Chokshi, Niraj. 2019. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next - The New York Times." https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html (July 22, 2019).

Clarke, Richard A. Richard Alan. 2010. *Cyber War: The next Threat to National Security and What to Do about It*. 1st ed. New York: Ecco.

Clarke, Richard A. Richard Alan, and Robert K. Knake. 2019. "What We Can Learn from the Most Damaging Cyberattack in History | LinkedIn." https://www.linkedin.com/pulse/what-we-can-learn-from-most-damaging-cyberattack-history-clarke/ (July 23, 2019).

Cook, Colonel James. 2010. "'Cyberation' and Just War Doctrine: A Response to Randall Dipert." *Journal of Military Ethics* 9(4): 411–423.

Dipert, Randall R. 2010. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9(4): 384–410.

Eberle, Christopher J. 2013. "JUST WAR AND CYBERWAR." *Journal of Military Ethics* 12(1): 54–67.

Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53(1): 23–40.

"Geneva Convention Relative to the Protection of Civilian Persons in Time of War." : 62.

Grosswald, Levi. 2011. "Cyberattack Attribution Matters Under Article 51 of the U.n. Charter." *Brooklyn Journal of International Law* 36(3): 1151–81.

Kinsella, David Todd, and Craig L. Carr. 2007. *The Morality of War: A Reader*. Boulder: Lynne Rienner Publishers.

Langner, Ralph. 2011. “Stuxnet: Dissecting a Cyberwarfare Weapon.” *IEEE Security & Privacy Magazine* 9(3): 49–51.

Newman, Lily Hay. 2018. “The Leaked NSA Spy Tool That Hacked the World.” *Wired*. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/ (August 3, 2019).

Nguyen, Reese. 2013. “Navigating ‘Jus Ad Bellum’ in the Age of Cyber Warfare.” *California Law Review* 101(4): 1079–1129.

“NSS 2018.Pdf.”

Schmitt, Michael N. 2014. “THE LAW OF CYBER WARFARE: QUO VADIS?” *Stanford Law & Policy Review* 25(2): 269–99.

Sklerov, Matthew J. 2009. “Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent.” *Military Law Review* 201.

Yusuf, Judge Abdulqawi A. 2012. “The Notion of ‘Armed Attack’ in the Nicaragua Judgment and Its Influence on Subsequent Case Law.” *Leiden Journal of International Law* 25(2): 461–70.