2018

R V E L O U S
N O V A T I V E
I L I M I T E D

TCGS

M N

V I

M A R V E L O
I N N O V A T I
U N L I M I T

General Assembly First Committee
Disarmament and international Security Committee
(DISEC)

Committee	General Assembly First Committee: Disarmament and International Security
Issue	Measures to Prevent Cyberwarfare
Expert Chair	Frank Chiu (IBST)

Introduction

The invention of the cyberspace has marked the beginning of a new era: the 4th Industrial Revolution. With technological advances and evolvements, the world has become a much smaller and closely-linked place. With the ability for the average person to communicate and relay information across the world in seconds, the rapid "transit" of information certainly makes this era one defined by an explosion of information aided by cyberspace.

The cyberspace has, undoubtedly, made society significantly more convenient. Never have communication and the access of information been so fast and available. However, like most other utilities, cyberspace is a double-edged sword. That is to say, in the hands of the wrong people, cyberspace could and has already become a dangerous weapon capable of sabotage or destruction on the national and international level.

Society has evolved fast: At first, the cyberspace was a military "weapon" and means of communication. It was hardly accessible to the average person. However, the commercialization of cyberspace has made it accessible to almost everyone, thus beginning an exponential increase in the amount of information exchanged on a daily basis. Individual hackers, long recognizing the many flaws inside this virtual world, started to hack to achieve malicious intents. It was only a matter of time before nations started picking up upon the practice, using cyberspace in ways unimaginable in the past: cyberwarfare.

In the simplest of its forms, cyberwarfare is "actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks." As this is a new yet urgent phenomenon, there

is a noticeable lack of international action regarding this subject. Although several solutions have been attempted, it is important to note a simple fact: cyberspace has become a new battlefield that is constantly evolving.

Definition of Key Terms

Cyberattack

"Any type of offensive maneuver employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts that either steals, alters, or destroys a specified target by hacking into a susceptible system." It is an umbrella term that includes cybercrimes, cyberterrorism, and cyberwarfare. Cybercrimes are criminal activities related or conducted through cyberspace. Cyberterrorism is the use of cyberspace to conduct acts of violence that impose a loss of life or significant bodily harm. Usually politically motivated, these attacks seek to intimidate and cause fear within populations.

Cyberwarfare

There have been extensive discussions over a proper definition of the actions that constitute cyberwarfare, with many different definitions provided by different parties. However, it is agreed universally that all acts of cyberwarfare share the following characteristics:

1. It is conducted through cyberspace.
2. The attack originates from a nation-state or international organization.
3. It is directed at another nation-state.
4. It attempts to damage computer or information networks by sabotage or disruption.
5. Physical damage to life, body, property etc. must be caused.
6. Under the circumstance of an attack, self-defense is invoked and justified.

Cyberspace

The virtual, interactive computer world. Unlike most technological jargons, cyberspace lacks a universal, standard, and objective definition. To this chair report, it is an “electronic medium used to form a global computer network to facilitate online communication.” Synonymous, but not identical, to the Internet.

Espionage

The act or practice of obtaining secrets (sensitive, proprietary, or classified information) from individuals, competitors, rivals, groups, governments and enemies for military, political, or economic advantage using illegal exploitation methods on the internet, networks, software and or computers. Synonymous, but not identical, to spying.

Hack

Any means of gaining unauthorized access to data in cyberspace.

Propaganda

Purposeful and deliberate dissemination of information to systematically influence and manipulate other people’s beliefs, attitudes, or actions in order to further an agenda or achieve a specific goal. Usually carries a negative connotation.

Warfare

Officially recognized as “acts of aggression”, as defined by the United Nations General Assembly Resolution 3314 (XXIX) in 1974, which includes the following:

1. There has to be destruction of life or property.
2. The intent and actions are of significance, not the result.

3. They can only be committed by a State or its agents.
4. The use of armed force.
5. They are against sovereignty, territorial integrity, or political independence.
6. Invasion, occupation, annexation, bombardment, blockade, attack on the land, air, or sea, state-supported attacks by non-state armed groups (NSAGs), etc.

Denial of Service (DoS) attack

Form of cyberattack that seeks to make a machine or network unavailable to its intended users includes disrupting services of a host connected to the Internet. Usually accomplished through flooding the target by a traffic of information to overload the system.

Background of the Topic

In June of 2013, Edward Snowden copied and leaked highly classified information from the National Security Agency (NSA), revealing to the public NSA's numerous global surveillance programs. Despite this incident being the first time national exploitation of cyberspace was sensationalized, it was far from being the first time cyberspace was compromised to achieve malicious intents by governments, non-state groups, companies, or individuals.

Interestingly, the concept of cyberwarfare was attributed to a short story, "Burning Chrome" by William Gibson, in 1982. Starting from the 1980s, the number of cyberwarfare has increased rapidly. According to the Professional Service Company, the number of cyberattacks jumped to 42.8 million in 2014, a 48% increase compared to 2013. Throughout this history, "nation-states and non-state groups have been using computer networks to strike, spy upon, or confound their adversaries."

The origin of cyberattacks could be traced back to 1988, when the first worms were created by Robert Tappan Morris. Named after the creator, the "Morris Worm" slowed 6,000 computers in the United States of America (USA) to the point in which it became unusable. It was after this incident that more institutions and organizations realized that they, too, were at the mercy of hackers. Soon, computer viruses have

evolved to achieve other purposes, for example, gathering and stealing information, disabling networks, etc.

Three major periods make up the history of cyberwarfare:

1. 1980s - 1998: Nations started to realize the potential harm in cyberspace. The USA and a few other nations started to develop offensive capabilities to confront hackers.
2. 1998 - 2003: Russia became another important actor in the cyber domain, and other nations started to pay attention to cyberspace, though these nations have not taken any action yet. Like the first period, the main focus of defense was against “hackers, hacktivist, and other non-state actors” rather than nations. In addition, cyberspace became an increasingly high priority in military exercises and activities.
3. 2003 - present: The cyberspace is now significantly more militarized, with a dramatic increase in the number of nations, for example, China, involved.

Throughout the three decades of cyberwarfare, there is, unfortunately, a large number of these attacks to serve as case studies. For example:

1. Aurora (2009): The first to have a large scale of influence, in Aurora, Chinese hackers systematically attacked a large number of US organization, including Google. US Secretary of State Hillary Clinton issued a public denouncement of China, the first public accusation made against nations instead of hackers and organizations.
2. Stuxnet (November 2007): Remaining as the most famous modern-day example of cyberwarfare, Stuxnet came at the shock of the international community. Essentially, it was allegedly a collaboration between the USA and Israel to undermine Iran’s nuclear weapon program. Not only was the hacking mechanism highly advanced, but it is also the first cyberattack to directly attack infrastructure.
3. Sony Pictures attack (2014): As a result of Sony’s controversial movie mocking North Korea’s leader, Kim Jong-Un, North Korea hacked Sony’s database, causing collateral damage to its commercialization.

Under the status quo, more than 140 nations have funded programs to develop cyber weapons. With the budget increasing year by year, nations are spending billions, while companies and other organizations are spending more than $10 million annually.

The rate of technological advancement is a direct causation of the increasing number of cyberattacks. As a result, countries have become aware that a cyberwar may take place in the near future. To combat this possibility, China, Israel, the USA, and the United Kingdom (UK) have invested the most to defense its cyberspace.

According to the Wall Street Journal (WSJ) in 2015:

1. “47 countries now have formal military or intelligence units dedicated to offensive cyber-efforts.”
2. “49 countries have bought off-the-shelf hacking software.”
3. “63 countries use cyber-tools for surveillance, either domestically or internationally.”

Key Issues

Popularity of Cyberwarfare

There are several structural reasons why cyberwarfare is especially popular and prevalent under the status quo:

1. The internet is very vulnerable to attack.
2. The cost of its imposition is low, i.e., the cost of hacking is low, but the return is high.
3. The lack of good defense systems against cyberattacks.
4. Everyone could participate due to the low barrier of entry, even terrorists.
5. Laws of war do not apply yet.
6. Disproportionate effect, i.e., Less Economically Developed Countries (LEDCs) and civilians are especially vulnerable to attacks.
7. It is hard to track the origin of attack, i.e., the cyberattacker could avoid incrimination.

Military Implications

Increasingly, the cyberspace is involved in military activities. In addition to the ability to wage cyberwarfare independently, cyberwarfare could be seen as a complement to current military operations in four ways:

1. Military data could be stolen and analyzed to predict and counter future operations.
2. Nations could intentionally downplay their military capabilities, causing opponents to relax.
3. False commands to troops could be given in lieu of top military commander.
4. Drones could be hacked to attack the originating side, forcing them to backfire.

For example, in 2013, Chinese hackers hacked the Pentagon, stealing “blueprints for some of the country's most sensitive advanced weapons systems,” including the advanced Patriot missile system (PAC-3), Terminal High Altitude Area Defense (THAAD), the Navy’s Aegis ballistic-missile defense system, F/A-18 fighter jet, the F-35 Joint Strike Fighter, the V-22 Osprey, the Black Hawk helicopter, and the Navy’s new Littoral Combat Ship.

Socioeconomic (Infrastructural) Damage

Attacks on critical state or privatized infrastructural integral to functionality have long been a concern for world leaders. Such attacks include the compromising, denial-of-service, sabotaging, or even taking direct control over power grids, telephone system, banking system, electricity and water systems, etc.

Differentiating itself from conventional warfare, these infrastructural attacks may prove to be much more damaging as cyberspace continues to develop. The strength of these attacks brings the ability to disable communication, coordination, and other resources necessary to conduct military operations. Without these components, a well-coordinated attack could easily clean-up what is left of the nation in question. Even if there are backup systems, it would take days to weeks to restore these services, a noticeable and fatal lag in defense. In addition, with the

transitioning to automation, many of such services are privatized and machine-run, meaning that there is less manpower to respond immediately to the emergency. What's worse, many of such private industries are not directly controlled by the government, therefore it is much harder to implement government regulations and defense mechanisms in these industries, rendering government intervention less effective.

However, the most detrimental effect of such cyberwarfare tactics is in the scope of its influence. National resources not only affect the army, but also civilians going on with their daily lives. A sudden shut-down of electricity, water, etc. translates to an impediment of economic activities, healthcare, education, and welfare systems. Economically speaking, billions and trillions could be lost in one attack, when years would be needed to fully recover from one. From a social standpoint, on the other hand, the impact on civilians is simply too large to comprehend and justify, as previous warfare focus significantly on disabling the military of the other side. Even if civilians were maimed in these previous conflicts, international treaties and laws with regards to these war crimes serve as checks and balances to such crimes.

The first example of such attacks is the December 2015 Ukraine power grid cyberattack, in which hackers were able to compromise three energy distribution companies in Ukraine and temporarily disrupt electricity supply for one to six hours. Despite the minimal impact, such attacks only served as a mere test, with experts and government officials citing the "huge potential impact" if such an attack were made with the most of malicious intents.

Espionage

The danger of espionage is subtle and obscure—precisely because it was supposed to be in the first place. The act of spying for political, military, or other types of information is illegal and severely punished under most legislation for good reason. The secretive and indiscernible harm of such attacks is hard to detect in the short-run, as no immediate threat is posed. This could be explained by analyzing the incentive of such attacks: unlike physical attacks on infrastructure, espionage is conducted to acquire information; thus, the longer the cyberattack could operate behind the scene, the more sensitive information could be stolen.

After such attacks, two main things could be done: First, the information could be kept to be analyzed, copied, or taken into account for future policies, making it a perfect complement with military implications (above). Second, the information could be used to blackmail or leak to the public to ruin the reputation of the organization or institution in question. For example, in the Sony attack, information on the racism that exists in the executive level was exposed. As another example, in 2014, eBay was hacked, resulting in the customers' name, encrypted password, email address, physical address, phone number, and date of birth of 148 million users being compromised. This is only one of numerous identity and password thefts to come. The credentials and trustworthiness of eBay are called into question; however, the true harm is the invasion of privacy and lack of security these millions of users experienced.

Propaganda

Cyberattacks do not merely exploit the weaknesses of network systems to achieve their malicious intents. Arguably, the human psychology has more weaknesses than that of network systems, as human emotions and perception are prone to change based on a plethora of factors. Also, humans remain as the ones that, if intended, could cause the most significant of harm. Most experts agree that technology, at least at the moment, is still a tool that humans use, regardless of intents. Thus, if the psychological weaknesses of humans are exploited, the individual could progress to cause more problems. Cyberattacks exploit the mental state of individuals mainly through political or social propaganda.

For example, according to the Federal Bureau of Investigation (FBI), Russian hackers used social media and other means of propaganda to potentially influence the results of the US Presidential Elections since 2012. As it explains, “The defendants allegedly conducted what they called information warfare against the United States, with the stated goal of spreading distrust towards the candidates and the political system in general.”

Major Parties Involved and Their Positions

China

The role China plays in cyberspace is controversial. Having the safest cyberspace in the world, China has been devoted to utilizing its potentials elsewhere, ranking first in the source of cyberattacks.

First, as a nation that actively censors the Internet and media to suppress dissent, China has developed its Great Firewall, isolating its population from the rest of the Internet. It is able to selectively let in information and exclude others. In addition, with its mass surveillance programs, all communications inside the nation are closely monitored.

Second, most of the recent and prominent acts of cyberwarfare have been traced to either Chinese state-sponsored cyberwarfare squadrons in the China's People's Liberation Army (PLA) or private, illegal hackers. The PLA alone has more than 100,000 hackers/soldiers, with its policy stating: "our warfare methods must adapt to the needs of information warfare… in this way, it will be entirely possible for China to achieve comprehensive victory over the enemy even under the conditions of inferiority in information technology." It is small wonder that China is allegedly accused of conducting cyberwarfare on countries including Australia, India, Canada, and especially the USA, with which China had the longest, most intense history of cyberwarfare and disagreements over information technology. According to the Department of Justice (DOJ), the majority of attacks against the USA originate from China. As it explains, "such cyber-attacks is 'an increasingly serious threat to US critical industries.'" Many believe that this aggressive behavior stems from the inferiority of China in military capabilities; therefore, in order to stabilize the imbalance of power, China must steal from "Pentagon's most sophisticated weapons systems" through corporate espionage to gain an advantage in cyberspace diplomacy by putting the USA on the defensive.

Politically speaking, China has denied all allegations of involvement in cyberwarfare. Their justification is simple: cyberattacks are illegal in China, so all hacks potentially from China are from private hacker groups that are operating illegally. As the spokesman of the Ministry of National Defense, Geng Yansheng

explained, “China’s laws ban any activities disrupting cyber security and Chinese government always cracks down on cyber crimes.”

On the international level, in September 2011, China proposed to the United Nations Secretary-General (UNSG) the “International Code of Conduct for Information Security,” which was heavily criticized for the potential censorship it creates. In addition, China has proposed to pass a new inclusive resolution to increase cyberpeace through creating a global solution to answer and defend against cyberwarfare by tracking down the creator of the attacks.

India

Despite its belated entry and realization of the need for a strengthened cyberspace, India is an emerging superpower in the technological and telecommunications field. With its growing reliance on technology, India has seen a significant increase in the number of attacks against its financial institutions and government. To combat security risks, India has implemented a national cybersecurity policy of 2013 (NCSP 2013), which cooperates with Japan and the USA to exchange information. The policy also marks the beginning of investing more resources and efforts into recruiting and training cyberspace professionals, including its first Chief Information Officer.

Iran

Ever since Stuxnet, Iran realized its cyberspace vulnerability and started to play an increasingly aggressive role in the field, developing its potential significantly. Its policy is closely aligned with the military Passive Defense Organization, which boasts the second largest cyber army and runs on an annual $76 million budget.

Israel

After a 2006 war against Hezbollah, a 2009 hacked internet during a military campaign in Gaza, and the “mass amount of conflicts Israel suffered with

neighboring nations," cybersecurity has become a top priority of the Israeli government, which has taken a thorough and critical approach in cyberspace. Consequently, Israel began to develop sophisticated technology and cyber- tactics while heavily monitoring vulnerabilities in their cybersystem and becoming actively involved in cyberwarfare planning, which involves citizens in the process.

Israel and the United States have both agreed to work constructively on cybersecurity. Although not explicitly stated, they have both agreed to work constructively on "cyberattacks" as well, such as developing Flame and Stuxnet together in the past. Over time, companies and nations have started to acknowledge the advanced role Israel plays in cyberspace.

Russian Federation

Similar in stance to China, the role Russia plays in cyberspace is also controversial.

Russia is one of the most prolific sources of cybercrimes in history, with the most infamous example being the Russian Business Network (RBN). As the largest cybercrime organization, it provides specialized services for malicious Internet users. Legally, Russia has banned any acts of cybercrime, tracking down and arresting such organizations. However, the difficulties these law enforcement agencies have to face have led some to suggest that these organizations enjoy state protection. For example, many cyberattacks have been traced back to Russian online platforms and forum, where criminal activities are discussed with impunity.

Historically, Russia was responsible for the numerous cyberattacks on eastern Europe, with Estonia and Georgia being the major victims. Over time, however, Russian cyber threat is becoming more significant than previously assessed. According to intelligence, Russian Ministry of Defense have already established its own cyber command responsible for such cyberattacks.

In terms of foreign policy, Russia has allegedly, under the orders of Vladimir Putin, launched a plethora of cyberattacks against Israel, Ukraine, the USA, the North Atlantic Treaty Organization (NATO), and the European Union (EU). Despite denying all state involvement in these attacks, there is concrete evidence of state sponsorship.

Russia's involvement in cyberspace has recently come to light during the US Presidential Election 2016, when investigations of Russian interference in the results of US elections are currently conducted. According to charges, Vladimir Putin ordered an "influence campaign" to damage Clinton's electoral chances and "undermine public faith in the US democratic process." With the recent firing of James Comey as the former director of the FBI and the indictment of 19 individuals and three companies by Robert Mueller, the already heated tensions between Russia and the US regarding the provision of refuge for Edward Snowden has elevated yet again. Regardless of the investigation results, these events serve as a turning point in the utilization of the cyberspace and a constant reminder of its influence.

It is therefore of great irony and controversy that Russia was the first country to take action to address cybersecurity, submitting a resolution to the UNGA First Committee in 1998. Being one of the first resolutions on this issue, it marked the first time cyberattacks were recognized as a significant challenge in the 21st century. The majority of these clauses aimed to encourage other countries to express their own views and positions on this topic, catalyzing an era of diplomatic engagement on this newly introduced subject. Soon after, other follow up actions were implemented, with Russia pushing for greater state control of the Internet.

Legally demanding a Russian information security monopoly, the Russian government is working on a new Cyber Security Policy to combat the growing issues with cyberspace. Among its priorities are "strengthening state guarantees of privacy, improving the competitiveness of Russian products, creating conditions for their wide use in the formation of national information systems and networks, as well as hardware and software crucial to maintaining information security of national information infrastructure facilities."

United States of America

As the nation of origin for the precursor of the Internet, ARPANET, the US military was quick to exploit the Internet to its fullest extent. Even today, the US has a considerable leverage over the Internet. With much information having to still flow through US servers, it is considerably easy for the government to intercept information at will.

Despite being the victim of most cyberattacks, the US is engaged in several controversial practices, including the interception of citizen communication, wiretapping, and its mass global surveillance program exposed by Edward Snowden.

However, when analyzed from a national security point of view, such activities are justified to the US government as part of its national defense program: as 9/11 caused a paradigm shift, after which developed nations could no longer take their safety and security for granted. Thus, from the US point of view, PRISM and the Five Eyes program are necessary responses to defend US national interests, a sovereign right. To the US, the impediment of US espionage programs is akin to sponsoring terrorism.

In addition, the US has a Five Pillar framework of cyberwarfare military strategy:

1. Recognition of this new type of warfare as being similar to existing battlespace arrangements.
2. The use of proactive defense instead of passive defense to defend against cyber threats.
3. The use of Critical Infrastructure Protection (CIP) to ensure the protection of critical infrastructure and systems.
4. The use of collective defense to enable early detection.
5. Maintain and enhance the growing technology to use as an advantage.

Timeline of Events and Relevant Documents

Date	Description of Event
1988	The first worm ("Morris Worm") is invented and spread by Robert Tappan Morris, significantly slowing 6,000 computers in the US.
1998	Russia introduces the first draft resolution regarding information security in the UNGA First Committee, which is adopted without a vote.
2009 - 2010	China conducts a series of cyberattacks against US-based companies in Operation Aurora.
November 23, 2001	Budapest Convention on Cybercrime is signed.
November 2007	Stuxnet is used to attack Iran's nuclear program.
September 12, 2011	China and Russia submit the "International Code of Conduct for Information Security" to the UNGA First Committee.
May 7, 2013	The Pentagon accuses China of extracting blueprints of US's most sensitively advanced weapons systems.
June 2013	Snowden leaks confidential NSA surveillance information.
May 21, 2014	eBay's database is hacked, with 148 million users' personal data being accessed and compromised.
November 24, 2014	Guardians of Peace (GOP) leaks confidential data from Sony Pictures.
December 23, 2015	Russia shuts down Ukraine's power grid temporarily.
May 2017 - present	Under Robert Mueller, the Special Counsel investigation on Russian interference in the 2016 US elections.

Analysis of Previous Attempted Solutions

Due to the relative late emergence of the issue, few concrete actions have been taken to address cyberwarfare. However, due to the increase of awareness on the issue, several solutions have been attempted and could serve as blueprints for future actions.

On an individual basis, many antivirus and computer security firms have flourished trying to prevent cyberattacks on the individual level. By installing firewalls and educating users about safe internet conduct, these companies try to significantly reduce the number of cyberattacks. Meanwhile, these large corporations themselves take significant caution and invest heavily in improving its security systems. For example, they employ white hat hackers to purposefully find flaws in their security systems. The problem, however, is that hacking techniques are constantly evolving to a higher degree of sophistication. Thus, none of these systems have a 100% success rate despite their constant development and improvements. These corporations also join forces with the local or national governments to adopt strategies for security. However, the lack of standardization and mandatory requirements in policing, and the controversy surrounding the balance of the invasion of privacy and national security interests both impede the process of producing a comparatively more effective solution. As shown in the Edward Snowden incident, checks and balances still need to exist on governments when exercising their authority.

On the national and international level, several nations, especially More Economically Developed Countries (MEDCs), have concrete cyberspace policies. However, these are not universally implemented and subjected to constant change. Some nations have tried to submit resolutions to combat the issue. Rarely, though, has there ever been unanimous or even majority support. The reason for this is simple: nations have different priorities in cyberspace. Some prioritize national security, while others do not wish to compromise individual freedom and privacy. Some regimes require a highly regulated national cyberspace to suppress dissent, which is met with strong opposition from Western liberal nations. Thus, despite the urgent need of a universal and efficient strategy to combat cyberwarfare, a consensus is hard to achieve. There is an interesting dilemma to note: if

anyinternational action is taken against the will of any sovereign nation, due to its non-binding nature and lack of enforcement, certain solutions specifically addressed at more cyber-aggressive nations would be rejected and be in vain. This illustrates the collective problem of these past international actions:

1. Three reports from the Groups of Governmental Experts (GGE)
2. Russian Federation's Convention on International Information Security, International Code of Conduct for Information Security, On the Developments in the Field of Information and Telecommunications in the Context of International Security
3. UNGA Resolution 57/239 (2003) regarding the "creation of a culture of cybersecurity"
4. UNGA Resolution 58/199 (2004) regarding discourse on strategies
5. UNGA Document A/70/174 regarding the definition of cyberspace norms and confidence building
6. Budapest Convention on Cybercrime regarding cybercrime, the harmonizing of national laws, improvement of investigative techniques, and cooperation
7. Laws of war, which includes Article 2 (4) and Article 51 of the UN Charter

The last solution attempted was defining warfare and acts of aggression and whether an act of self-defense in response to cyberwarfare is legal and justified. Article 2 (4) bans armed forces, while Article 51 was vague in defining weapons. Thus, much controversy and arbitrary interpretations of international law still exist under the status quo.

Possible Solutions

Cyberspace will always be an ever-evolving and volatile field. Thus, when talking about this field, there is always room for improvement and new discoveries. With that being said, the simplest solution to cyberwarfare is to constantly update technological programs of private sectors and government institutions. However, as hacking techniques are always constantly evolving, simply updating infrastructure would only be a short-term solution. In short, it would turn out to be a never-ending cycle as both attackers and defenders mature and progress.

Another way to approach this issue is to attempt to regulate cyberwarfare and start the disarmament process. This would require a new and universal definition of warfare. With a new definition, it would be easier to take action, classify types of cyberwarfare, and determine whether a military response is necessary on a case-by-case basis. A possible definition of cyberattacks constituting cyberwarfare is effect-based: once a cyberattack leads to a physical harm, it would be deemed as an act of war. Of course, this definition is up for debate as it is by no means perfect and would violate the stances of some nations.

However, change must also start at a smaller level. In order to combat cybercrimes and eventually warfare within nations, it is important to start with education and raising awareness. State support for research, training of defensive professionals and policing efforts could be used to combat these criminal activities.

On an international level, nations could cooperate and negotiate through a variety of platforms. Transparency of issues for both citizens and nations is integral to trust and further willingness to help in discourse about problems and solutions.

Bibliography

"Cyberspace: The New Battlefield?" Cyberspace: the New Battlefield? | CIPADH, 26 Feb. 1970, www.cipadh.org/en/cyberspace-new-battlefield.

"What Is a Cyberattack? - Definition from Techopedia." Techopedia.com, www.techopedia.com/definition/24748/cyberattack.

"What Is Cyberwarfare? - Definition from WhatIs.com." SearchSecurity, www.searchsecurity.techtarget.com/definition/cyberwarfare.

"What Is Cyberspace? - Definition from Techopedia." Techopedia.com, www.techopedia.com/definition/2493/cyberspace.

"United Nations Audiovisual Library of International Law." United Nations, United Nations, www.legal.un.org/avl/ha/da/da.html.

Dunn, John E. "The World's 10 Most Dangerous Cyberwarfare Attacks." Techworld, 14 Mar. 2015, www.techworld.com/security/worlds-10-most-dangerous-cyberwarfare-attacks-3601660/.

Greenberg, Andy. "'Crash Override': The Malware That Took Down a Power Grid." Wired, Conde Nast, 13 June 2017, www.wired.com/story/crash-override-malware/.

McCarthy, Tom. "Ten Key Takeaways from Robert Mueller's Russia Indictment." The Guardian, Guardian News and Media, 16 Feb. 2018, www.theguardian.com/usnews/2018/feb/16/russians-indictment-mueller-charges-fbi-investigation-what-are-they.

Montierth, Adam Greer and Nathan. "How Are US-China Cyber Relations Progressing?" The Diplomat, The Diplomat, 2 Nov. 2017, www.thediplomat.com/2017/11/how-are-us-china-cyber-relations-progressing/.

Skroupa, Christopher P. “Cyber Warfare -- Reasons Why Israel Leads The Charge.” Forbes, Forbes Magazine, 7 Sept. 2017, www.forbes.com/sites/christopherskroupa/2017/09/07/cyber warfare-reasons-why-israel-leads-the-charge/#489f9fcf6e36.

Stavridis, James. “How to Win the Cyberwar Against Russia.” Foreign Policy, Foreign Policy, 12 Oct. 2016, www.foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

Affairs, Ministry of Foreign. “The Budapest Convention on Cybercrime: a Framework for Capacity Building.” News Item | Global Forum on Cyber Expertise, Ministry of Foreign Affairs, 5 Dec. 2016, www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime.