Forum: Commission on Science and Technology for Development

Issue: Addressing the threat of cyberwarfare, cyber terrorism, and espionage

Student Officer: Isaac Zenko

Position: Deputy President

Introduction

As the decades pass and the years roll over to the next, the complexity of the status quo diversifies into branches of ever-winding and ever-growing awareness. At the end of the 20th century, a new era of human innovation was born as circuits and mechanisms formed the intricate works of the computer system. With this conception, an unfamiliar landscape of warfare came along, replacing bullets and artillery with lines of code. The regular means of warfare have shifted into the cyberspace of the Internet. Cyberwarfare should not be taken lightly, as it has been the ground of many causes of economic disruptions, financial theft, breaches of national security, removals of classified information, and violations of individual privacy. This method of warfare is usually carried out by nation-states and governments. However, with the spread of technology worldwide, non-state actors and individuals came to have the power to cause undesirable effects on the economy, society, and government. Therefore, a plan of action must be devised to hinder or at least address the Internet's use to threaten privacy and security.

Definition of Key Terms

Cyberwarfare

the use of technology and computer networks as a strategic domain for conducting warfare, involving offensive and defensive operations in the digital realm and targeting the computer systems, networks, and information infrastructure of an adversary, thereby gaining strategic advantage, which primarily goes on between state actors.

Cyberterrorism

the use of computer systems and the Internet by individuals or groups with the intention to instill fear, cause harm, and/or promote ideological, political, or religious agendas by exploiting digital systems, networks, and information infrastructure to carry out acts of terror and create disruption on a large scale.

Cyber espionage

the covert gathering of sensitive or classified information from computer networks, systems, or digital devices of individuals, organizations, or governments, involving the use of cyber tools, techniques, and methodologies to infiltrate and extract valuable intelligence or proprietary data.

Cyber propaganda

the dissemination of misleading, manipulative, or biased information through digital platforms with the intention to shape public opinion, influence perceptions, or advance specific agendas, primarily through online channels, social media platforms, websites, and other digital mediums to spread propaganda messages and narratives.

Cybersecurity

the practice of protecting computer systems, networks, and data from unauthorized access, use, disclosure, disruption, or destruction by implementing measures to prevent, detect, respond to, and recover from cyber threats.

Cyber threat

any potential event, action, or situation that has the potential to compromise the confidentiality, integrity, or availability of computer systems, networks, or digital data, encompassing a wide range of malicious activities, vulnerabilities, and risks in the digital domain.

Threat actors

individuals, groups, or entities that engage in cyber activities with malicious intent, including nation-states, criminal organizations, hacktivist groups, terrorists, or insider threats.

Advanced Persistent Threats (APTs)

long-term, sophisticated state-sponsored cyber espionage campaigns involving targeted attacks, social engineering, and advanced hacking techniques that are often well-funded, persistent, and focused on specific targets of interest.

State-sponsored actors

individuals, groups, or entities that are actively supported by a government or a state entity to enact a specific goal.

State-sponsored cyberwarfare

cyber operations that are conducted or supported by a government or a state entity to target other nations, organizations, or individuals and are often carried out for political, military, economic, or intelligence purposes.

Hacktivist

individuals who carry out cyberattacks in support of political, religious, or ideological causes.

Malware

software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Jus ad bellum

the international law that regulates the right of war by one state on another.

Jus in bello

the international law that governs the conduct of belligerents during war in order to mitigate unnecessary damage and suffering.

Background

The foundations of cyberwarfare can be traced back to the development of early cybernetics and information theory around the 1940s to 1950s. Pioneers like Norbert Wiener and Claude Shannon laid the groundwork for understanding communication and control in machines and biological systems.

However, the landscape of cyberwarfare started to take shape around the 1950s to 1960s during the Cold War era, when the United States and the Soviet Union engaged in a geopolitical rivalry. While the term "cyberwarfare" was not in use during that time, the development of computer technology and its integration into military operations laid the groundwork for the modern concept of cyberwarfare. The United States and the Soviet Union explored the use of computers in strategic planning, cryptography, and communication.

In 1969, the United States Department of Defense (DoD) developed the Advanced Research Projects Agency Network (ARPANET), the precursor to the modern Internet. Initially designed for resilient and decentralized military communication in the event of a nuclear attack, ARPANET laid the foundation for interconnected computer systems. The Soviet Union also invested in computer networks for military purposes, albeit with different technical approaches. They sought to enhance command and control systems and improve communication and coordination among military units, especially in response to the perceived threat from the United States and its NATO allies.

The 1980s witnessed the emergence of early cyber espionage and hacking incidents. The famous case of the WANK worm in 1989 targeted NASA's SPAN network, highlighting the vulnerability of computer systems. With the increasing reliance on information systems, the 1990s saw a shift towards the concept of "information warfare." Nations started recognizing the potential of using cyber capabilities in conflicts. The Stuxnet worm, discovered in 2010, marked a turning point in cyberwarfare. It was a sophisticated malware designed to target Iran's nuclear facilities, and its discovery highlighted the potential for cyber weapons on a global scale.

The Range of Cyberthreat and Cyberterrorism

Technology has spread across the world to every nation. As access to the Internet becomes generalized, unwanted people gain access and take advantage of it. Since cyberspace is interconnected throughout the world, people with the proper understanding of it have the power to navigate it. Individuals may have malicious intent with a particular country and use their knowledge of the Internet to disrupt specific government computer systems. These individuals with certain political, religious, or ideologies may form groups and utilize cyberspace to propagate their beliefs. Such groups include terrorist organizations like Al-Qaeda, ISIS, and Anonymous. These terrorist organizations pose a significant threat to the cyberinfrastructure, computer systems, and digital information of nations worldwide. Some nations pose a threat to other states with cyberwarfare. With nations, their range of power in cyberspace is internationally supported and well-funded, with cyber experts and a wide field of tools at their disposal.

The History of Cybersecurity

Malicious entities try to cause havoc and gain classified information from nations, firms, and individuals. However, there are cybersecurity professionals who work to improve the cybersecurity of computer systems and networks by conducting ethical hacking. Cybersecurity acts as the defensive system of cyberspace. The concept of cybersecurity testing started in 1971 with a computer programmer named Bob Thomas. He created a non-malicious self-replicating worm virus called “Creeper” as an experimental program to test the ARPANET created by the US government as the foundation of the modern Internet. Creeper would spread all throughout the computer networks, infecting and corrupting mainframe computers. As a result, it can call attention to security flaws and areas of vulnerability and exposure in the ARPANET. In 1995, John Patrick, Vice President of the International Business Machines (IBM) Corporation, coined “ethical hacking” and provided a platform for those “ethical hackers.”

Past Examples of Cyberattacking Operations

Moonlight Maze (1996)

Moonlight Maze was one of the earliest known instances of state-sponsored cyber espionage, starting in 1996 and ending in 1997. It involved a series of intrusions into U.S. military and research networks, with suspected origins in Soviet Russia, as the tracked IP address originated from the region. The attackers targeted classified information of the American government, affecting NASA, the Pentagon, the Department of Energy (DOE), the military, and numerous other American government agencies. Moonlight Maze was classified as an Advanced Persistent Threat (APT).

Titan Rain (2003)

Titan Rain was a series of cyber espionage attacks in 2003 that targeted various U.S. government agencies, defense contractors, and other organizations. The campaign was first publicly reported in 2005 and drew significant attention due to the scale and sophistication of the attacks. The attackers behind Titan Rain were believed to be state-sponsored actors, with China often being identified as the suspected source, aiming to

infiltrate computer networks and steal sensitive information, particularly defense and national security. The exact duration of these attacks is not disclosed.

Operation Olympic Games, aka Stuxnet (2006)

Operation Olympic Games, also known as Stuxnet, refers to a covert cyber operation that targeted Iran's nuclear program, which started in 2006 and continued until 2014. It was a joint effort between the United States and Israel, which aimed to disrupt Iran's uranium enrichment activities. It involved using a sophisticated malicious computer worm called Stuxnet, specifically targeting industrial control systems, such as those used in Iran's nuclear facilities. Stuxnet aimed to cause physical damage to the equipment and disrupt Iran's nuclear program without arousing suspicion by exploiting vulnerabilities in Windows operating systems and Siemens supervisory control and data acquisition (SCADA) systems, which were commonly used in Iran's nuclear infrastructure, to tamper with the centrifuge operations. The operation reportedly set back Iran's nuclear efforts for several years. Its existence was first publicly reported in 2010.

The Estonia Cyber Attacks in 2007

The 2007 Estonia Cyber Attacks, also known as the "Bronze Soldier" or "Web War I," was a series of cyberattacks that started on April 27, 2007, targeting Estonia's governmental, financial, and media institutions. The attacks, which were believed to be orchestrated by Russia, disrupted Estonia's online services and highlighted the potential impact of cyberwarfare on a nation. The cyberattacks were rooted in a dispute over relocating a Soviet World War II memorial, the Bronze Soldier statue, from the center of the capital, Tallinn, to a military cemetery. The decision sparked protests and tensions between Estonia and Russia, as it was a sensitive issue related to historical and political perspectives. The cyber attacks involved distributed denial of service (DDoS) attacks, defacement of websites, and various forms of online harassment. The targeted entities included Estonian government websites, financial institutions, media outlets, and other organizations. The attacks aimed to disrupt Estonia's digital infrastructure, cripple online services, and undermine the country's stability.

Operation Aurora (2009)

Operation Aurora, also known as the Google Aurora attacks, was a cyber espionage campaign originating from China targeting several major technology companies, including Google, Adobe Systems, Rackspace, Akamai Technologies, Yahoo, and Juniper Networks, from June to December 2009. The primary objective of Operation Aurora was to gain unauthorized access to the networks of targeted companies and steal intellectual property, trade secrets, and other sensitive information to exploit vulnerabilities in popular software applications. The operation came to light when Google publicly disclosed the attacks in January 2010, stating that it had been targeted and that intellectual property had been stolen.

Duqu

Duqu is a sophisticated and stealthy computer malware discovered on September 1, 2011. It is closely related to the Stuxnet worm and shares some of its code and techniques. Duqu is often referred to as a "sibling" or "cousin" of Stuxnet due to their similarities in design and purpose. It was primarily used to target organizations and entities involved in critical infrastructure sectors, such as energy, telecommunications, and industrial control systems. The creator of Duqu is unknown but is speculated to be the United States and Israel.

Flame (2012)

Flame, also known as Flamer or Skywiper, was a highly sophisticated cyber espionage malware that primarily targeted systems in the Middle East, with a focus on governmental organizations, research institutions, and critical infrastructure sectors such as energy and telecommunications in 2012. The malware infected Israel, Palestine, Sudan, Syria, Lebanon, Saudi Arabia, Egypt, and primarily Iran. The exact origins of Flame are unknown. However, there is speculation that it is a joint effort between the United States and Israel since Flame shares very strong similarities with Stuxnet and Duqu.

WannaCry (2017)

WannaCry is a notorious ransomware attack that occurred in May 2017. It spread rapidly across the globe, affecting hundreds of thousands of computers in over 150 countries. The attack targeted computers running Microsoft Windows operating systems, exploiting a vulnerability in a Windows protocol. WannaCry was unique because it incorporated elements of both ransomware and worm-like behavior. It encrypted files on infected systems, rendering them inaccessible, and demanded a ransom payment for the decryption key. The ransomware could also self-propagate and spread to other computers on the same network, rapidly increasing its proliferation. WannaCry garnered significant attention and impact due to its widespread disruption, affecting critical infrastructure, government agencies, healthcare organizations, and businesses worldwide. It notably affected the UK's National Health Service (NHS), causing the cancellation of appointments and the temporary shutdown of some healthcare services. The attack was attributed to the North Korean state-sponsored hacking group Lazarus Group, based on similarities in code and infrastructure used in previous attacks attributed to this group. The motive behind the attack was believed to be financial, as the ransom payments were directed to Bitcoin wallets associated with the attacker.

NotPetya (2017)

NotPetya is a destructive ransomware attack initially believed to be a variant of the Petya ransomware; however, further analysis revealed that it was a distinct malware with worm-like spreading capabilities. Petya first emerged in Ukrainian companies on June 27, 2017, including the National Bank of Ukraine, but quickly spread to various countries worldwide, including Russia, France, Germany, Italy, Poland, the United Kingdom, and the United States, affecting organizations across multiple sectors, including government agencies, banks, energy companies, transportation systems, and critical infrastructure. It caused significant disruption and financial losses. Even though it affected Russia by a tiny amount, there

was reason to suspect that Russia was the one that planted NotPetya in Ukrainian companies; it was attributed to state-sponsored actors, specifically the Russian military. Many were convinced that this was a geopolitically motivated attack against Ukraine since it occurred on the eve of Constitution Day in Ukraine.

SUNBURST (2020)

The SolarWinds supply chain attack, or SUNBURST, was a major cyberattack that started in March 2020 and discovered in December 2020 that compromised SolarWinds' software and led to a significant supply chain breach affecting numerous organizations, including government agencies, defense contractors, technology companies, critical infrastructure providers, and private companies, such as Intel, Cisco, and Palo Alto Networks. The attack involved inserting a malicious code into SolarWinds' Orion software used for network and IT infrastructure management. It enabled them to move laterally within the networks, escalate privileges, and exfiltrate sensitive information. The attack went undetected for several months, highlighting the level of sophistication and stealth employed by the attackers. US government departments were affected, including the Department of Defense, the Treasury Department, and the Department of Homeland Security. This attack was widely attributed to a state-sponsored hacking group believed to be linked to Russia, named APT29 or Cozy Bear. The motive behind the attack is believed to be espionage and intelligence gathering.

Major Parties Involved

The United States of America (USA)

As one of the greatest military powers of the world, the United States of America has been the leading nation in the field of cyberwarfare. The USA supports the use of technology and computer networks to conduct cyberattacks on other nations and non-state actors, endorsing the militarization of cyberspace. However, they are against non-state actors, such as terrorist groups and hacktivists, performing cyberattacks. Along with the Soviet Union during the Cold War, the USA pioneered the first offensive and defensive cyber operations against each other. The US government has suffered from several cyberattacks and carried out cyberattacks on other parties by state-sponsored entities, especially by the US military, in the past. They have been targeted by China and Russia, which were trying to gain classified government information, as the US has done with Middle Eastern countries and other rival countries with cyber espionage operations such as Operation Olympic Games, which saw a collaboration with Israel against Iran.

In the 1990s, scholars from the UK and the USA came together and proposed the concept of "cyber power," which is a country's ability to impact and take measures in cyberspace. The White House published an "International Strategy for Cyberspace" in 2011 that advocated for the right to use military force in response to cyberattacks, as they regard cyberspace attacks the same as other types of threats and as an act of war. In July 2011, the U.S. Department of Defense (DoD) took measures to develop capabilities to defend the nation against

cyberattacks, publishing the DoD Strategy for Operating in Cyberspace. In April 2015, they built upon the DoD Strategy for Operating in Cyberspace to form the DoD Cyber Strategy. As part of the DoD, the United States Cyber Command (USCYBERCOM) focuses on cyber threats. The National Security Agency (NSA) is also an essential entity responsible for cyber activities.

The Russian Federation

Russia was another pioneer of cyberwarfare due to its Cold War with the USA when it was still called the Soviet Union. They have conducted cyberattacking operations on various nations, including Estonia, France, Germany, the United Kingdom, Poland, and South Korea. But the most notable instances of these attacks were targeted towards the USA and Ukraine. From 1969 to 1999, the first Russian cyberattack against the USA was discovered and called Moonlight Maze, which infiltrated the backdoor systems of NASA, the Pentagon, the US military, and other government agencies. Additionally, as there were growing tensions between Russia and Ukraine, multiple cyberattacks on Ukraine were discovered, which started in 2010 with a Russian cyber weapon called Snake or "Ouroboros" that disrupted Ukraine's government systems. With the now-raging Russo-Ukrainian War, Russia's cyberwarfare systems have never been more active, targeting critical infrastructure like power grids.

Many nation-states regard Russia as a cyber threat, as Russia would continue to focus on improving its cyber technology further in offensive and defensive situations. Russia certainly wants to keep its dominance in the field of cyberwarfare but is opposed to its use by hacktivists and cyber-criminal syndicates. Russia's principles on cybersecurity and warfare are deeply rooted in Soviet-era tactics, incorporating both technical and psychological weapons in its arsenal. Information on Russia's range of cyber technology and warfare is limited due to their uncommunicative nature on their militaristic aims.

The People's Republic of China (PRC)

China has been recognized as one of the principal actors in the field of modern cyberwarfare. Its involvement in cyberwarfare can be traced back to the late 1990s, and since then, it has significantly developed its cyber capabilities as the Chinese economy has improved over the decades, especially in the industry of technology. One of the earliest known cyber espionage incidents associated with China was the "Titan Rain" operation in the early 2000s. It targeted the U.S. government and defense networks, emphasizing China's interest in acquiring military and technological information. China has been linked to several Advanced Persistent Threat (APT) groups responsible for conducting cyber espionage campaigns. In the late 1990s, China established the "NET Force" unit within the People's Liberation Army (PLA) to focus on cyber operations. The PLA Strategic Support Force (SSF) is responsible for coordinating China's military cyberspace operations, including offensive and defensive cyber capabilities.

Like Russia, many nations see China's involvement in cyberwarfare as a significant threat to the security of cyberspace. On the one hand, China disapproves of insensibly giving undue importance to the significance of cyberwar; on the other hand, it strives to promote stimulating discussions by participating in academic dialogue and exchange with its international peers. In 2009, bilateral discussions were held between China and Japan about joint

research on the idea of "Hegemony in the Internet Era." They delved into and advanced the notion of "cyber power" proposed by UK and US scholars. China's stance firmly opposes the militarization of cyberspace and endorses revision and clarification of existing international law so they apply to cyberspace. However, it is difficult to determine whether China truly upholds its stance since evidence of several cyberattack groups has led back to the Chinese government.

The Democratic People's Republic of Korea (DPRK)

Despite North Korea's limits in technology and resources, it has been an active threat to the rest of the international world because of its state-sponsored hacker training program situated in mainland China called the Lazarus Group. The Lazarus Group has been attributed to various instances of cyberattacks and cyberespionage, including the 2013 South Korean cyberattack, the 2014 Sony Pictures breach, the 2017 WannaCry ransomware attack, and the 2020 pharmaceutical company attacks. A majority of these cyberattacks aim to fund its regime. This includes hacking banks and cryptocurrency exchanges to steal these funds. The rest of these cyberattacks aim to spy on vital information from other countries, targeting South Korea and other nations, their government agencies, military organizations, and defense contractors. The Lazarus Group is known for employing various types of malware to achieve their objectives, which affected organizations worldwide.

The North Korean government is believed to be directly involved in orchestrating and supporting cyber operations. The Reconnaissance General Bureau (RGB), a North Korean intelligence agency, is suspected of playing a significant role in coordinating these cyber activities carried out by the Lazarus Group. North Korea does not have an official public stance on cyberwarfare as of today. However, by seeing its activity in this domain, it is certain that North Korea endorses the militarization of cyberspace.

The Republic of Korea (ROK)

Given its geopolitical situation and the prevalence of cyber warfare in the region, South Korea has been actively involved in addressing and responding to cyber threats. South Korea has faced cyber threats from various actors, especially North Korea. South Korea has been a target of cyberattacks from North Korea, and there have been incidents of cyber espionage and other malicious activities attributed to the North Korean hackers, the Lazarus Group. Notable attacks on South Korea include the 2013 South Korean cyberattack and the 2014 Sony Pictures hack conducted by the Lazarus Group.

The South Korean government has taken steps to enhance its cyber capabilities and collaborate with international partners to address cyber threats. This includes participating in joint cybersecurity exercises and information sharing with other nations. South Korea has implemented comprehensive cybersecurity policies and measures to protect its critical infrastructure, government networks, and private sectors from cyber threats. The Korea Internet & Security Agency (KISA) is the government agency responsible for cybersecurity in South Korea. South Korea has naturally taken a somewhat antagonistic stance on cyberwarfare but has not made its official public stance on the matter yet.

The Islamic Republic of Iran (IRI)

Iran is regarded as a developing military power in cyberwarfare. Iran's cyber capabilities have evolved, reflecting a broader recognition of the role of cyber warfare in national security. Iran's history in cyber warfare is marked by its involvement in various activities, including cyber espionage, disruptive attacks, and efforts to enhance its cyber capabilities. The nation has been linked to several Advanced Persistent Threat (APT) groups believed to be state-sponsored, engaging in cyber espionage campaigns with geopolitical objectives. The country's involvement in disruptive cyber attacks, such as the 2012 Shamoon malware attacks against Saudi Aramco, demonstrates its willingness to employ cyber tools for strategic and geopolitical purposes. Iran also experienced the Stuxnet worm in 2006, a cyber weapon believed to be developed jointly by the United States and Israel, which targeted Iran's nuclear facilities.

Iran's stance on cyber warfare reflects its acknowledgment of the strategic importance of cyberspace in modern conflicts, recognizing the potential of cyber capabilities for both offensive and defensive purposes and utilizing cyberwarfare as a part of its "soft war" military strategy. Since November 2010, Iran established "The Cyber Defense Command," a subdivision of the "Passive Civil Defense Organization," which is a subdivision of the Iranian Armed Forces, to provide defensive operations for cyberwarfare. As international tensions persist, Iran's stance on cyber warfare will likely remain a dynamic aspect of its overall security strategy, with ongoing developments contributing to the complex landscape of global cyber threats.

The State of Israel

Israel is considered to have a solid ground in the field of cyberwarfare. It is known for its advanced cyber capabilities and has been involved in cyber operations focusing on intelligence gathering and countering security threats. Israel's history in cyber warfare is marked by its active engagement in addressing emerging threats and adapting to the evolving cyber landscape. The country has reportedly been involved in offensive cyber operations aimed at disrupting adversaries' activities and gathering intelligence. Notably, Israel is credited with the development of the Stuxnet worm, a cyber weapon designed to target Iran's nuclear facilities in 2006 in collaboration with the United States. Israel's ongoing investment in cyber research and development, coupled with its proactive approach to cybersecurity, positions the nation as a formidable player in the global cyber landscape.

Israel maintains a strategic and proactive stance on cyber warfare, recognizing the significance of cyber capabilities in modern conflict. With a robust cyber defense strategy, Israel places a high priority on safeguarding its critical infrastructure and countering cyber threats. The country is renowned for its advanced cyber capabilities, and its military intelligence unit, Unit 8200, plays a pivotal role in conducting cyber operations, intelligence gathering, and responding to security challenges in cyberspace. Israel has consistently demonstrated its commitment to innovation in cybersecurity, fostering a strong cybersecurity ecosystem that includes both governmental and private-sector entities. The nation's focus on cutting-edge technologies and collaboration between government agencies and industry stakeholders underscores its commitment to staying at the forefront of cyber defense. However, with the current war between Israel and Palestine, Israel is in a challenging position to set everything straight again.

Timeline of Events

Date	Description of event
1940s-1950s	People like Norbert Wiener and Claude Shannon lay the groundwork for understanding communication and control in mechanical and biological systems by developing early cybernetics and information theory.
1950s-1960s	The United States and the Soviet Union explores the concept of cyberwarfare as part of their Cold War rivalry. This leads to the development of offensive and defensive capabilities.
1969	The United States Department of Defense (DoD) develops the Advanced Research Projects Agency Network (ARPANET), which is designed for efficient military communication and laid the foundation for the Internet and interconnected computer systems.
1971	Bob Thomas creates the Creeper malware to test out the ARPANET's vulnerabilities.
1980s	The emergence of personal computers and interconnected networks lays the groundwork for the future of cyber conflict. Cyber incidents started to emerge; however, cyber incidents during this period were relatively limited in scale and sophistication.
1989	The WANK worm in 1989 targets NASA's SPAN network.
1990s	The concept of "information warfare" emerges with the increasing reliance on information systems and networks. During this time, nations start to recognize and address the problems with cyberspace and its potential uses in conflicts.
1996	The cyberattacking operation called Moonlight Maze attacks U.S. military and research networks, originating from Soviet Russia. It is one of the earliest known instances of state-sponsored cyber espionage.
2006	The Stuxnet worm enters into operation as a sophisticated malware created by a partnership between the U.S. and Israel to target Iran's nuclear facilities. Its discovery in 2010 highlighted the potential for cyber weapons on a global scale, marking a turning point in cyberwarfare. It continued until 2014.
27 April 2007	A series of cyberattacks led by Russia targets Estonia's governmental, financial, and media institutions, disrupting various online services. This highlighted the potential impact of cyberwarfare on a nation as the first case of a national-level cyberattack.

Previous Attempts to Resolve the Issue

In 1999, Russia proposed "principles of international information security" to the UN Secretary-General, but this proposal received little support. In 2004, a United Nations Group of Governmental Experts (GGE) was created for nations to engage in discussions about and develop norms for responsible state behavior in cyberspace for the purpose of international security. Since then, six GGEs have been established. The 2019-2021 GGE was created on 2 January 2019 by the UN General Assembly's (GA) resolution 73/266. However, despite the 2019-2021 GGE's difficulty in reaching a consensus on specific norms and rules, they submitted UN report A/76/135 in 2021 on "Advancing responsible State behaviour in cyberspace in the context of international security." UN compendium A/76/136 of the GGE's report in 2021 was published on 15 states and how information and communications technologies (ICTs), in regard to international law, apply to each of these states. However, the most notable progress was the 2013 UN consensus report A/69/98, which outlined a set of cyber norms and reaffirmed international law, state sovereignty, and human rights regarding cyberspace. In 2015, the GGE submitted UN report A/70/174, which expanded on the principle of nonintervention in internal state affairs and highlighted that states should protect their own critical infrastructure and should refrain from carrying out cyberattacks that damage critical infrastructure. The 2015 developments have provided a foundation for subsequent norm discussions on cyberspace and cyberwarfare. These UN documents are comprehensive pieces that must be read to reflect the same thoroughness in your resolution.

The UN Open Ended Working Group (OEWG) on Information and Communication Technologies (ICTs), created by UN resolution A/C.1/73/L.27/REV.1, which was a Russia-sponsored resolution, attempted to oversee state operations and behavior in cyberspace with regulations to maintain international peace and security. It adopted UN consensus report A/AC.290/2021/CRP.2 in March 2021. There has been great discord between the USA and its allies with Russia and China and their allies. Thus, the OEWG process has led to an impasse.

The *Tallinn Manual* was written between 2009 and 2012 by an international group of about twenty experts, legal scholars, and practitioners assembled by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) to address how to apply international law, the *jus ad bellum*, and the *jus in bello* in the context of cyber warfare. Cambridge University Press released Tallinn 2.0 to expand on what the *Tallinn Manual* sought to accomplish, specifically touching on issues with cyber operations rather than cyberwarfare.

The GA of the UN has many resolutions regarding this topic. The UN GA's resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, and 63/37 of 2 December 2008 addressed developments with respect to information and telecommunications in the context of international security. The UN GA's resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 engage in combating the criminal misuse of information technologies, 57/239 of 20 December 2002 address the creation of a global culture of cybersecurity, and 58/199 of 23 December 2003 and 64/211 of 21 December 2009 address the creation of a global culture of cybersecurity and the protection of critical information infrastructures.

Many reports by cybersecurity firms and governmental organizations have detailed the possible solutions for the issue of cyberwarfare and cyberthreats, including the U.S. Department of Defense (DoD) and Cybersecurity & Infrastructure Security Agency (CISA).

Possible Solutions

Global standards on the issue of cyberwarfare have always maintained the objective of holding international discussions, establishing international and domestic law, leading competent investigations, increasing public and global awareness, facilitating information transparency and academic exchanges, and sharing best practices. However, it is disputed among the countries whether cyberwarfare and cyberweapons should be banned internationally since the idea of completely prohibiting cyberwarfare is polarized. Those countries that are significant actors in the field, including all the P5 nations, want to preserve their power in cyberspace. Thus, they are against the prohibition of state cyberwarfare as a whole. However, countries differ in stance on whether non-state-sponsored entities should be allowed to conduct cyberattacks and cyberespionage. Furthermore, it is widely agreed that cyberterrorism should be prohibited in any shape or form.

There will always be fundamental disagreements among states, with three main categories of states: the USA's allies, Russia and China's allies, and "swing states," which are mainly composed of developing countries. "Swing states" have largely not committed to discussions and debates on cyberwarfare and cyber norms. China and Russia have advanced the concept of "information sovereignty," especially to "combat false news," which has sparked up large disputes between the two major sides of member states since the US side of things was to strive for an "open, reliable, and secure information environment."

Setting up international law in cases before, during, and after cyberwar is crucial in creating a thorough resolution. The *jus ad bellum* and *jus in bello* regarding cyberwarfare must be established and expanded upon from existing international law and resolutions. Perhaps cyber ceasefires can be implemented during cyberwars. It is also crucial to address international humanitarian law due to the lack of reference to this issue in existing settlements.

Transparency among nation-states and their endeavors in cyberspace will facilitate meaningful cooperation internationally. Such exchanges between nations should include discussions on innovations and discoveries in the field, advancing systems of offensive and defensive operations, and joint research surrounding cyberwarfare. Within such discussions, technical issues must always be consulted with an expert in the field. With developing countries such as Indonesia, India, and South Africa, the urgent need for information exchange on technical issues, especially cybersecurity measures, increases since these nations do not have adequate defense against or even detection systems for powerful cyberattacks.

Sanctions and reparations may also be imposed on those countries that conduct significant damage to another; however, such a solution will cause much discord because nations may not agree with sanctions as a whole as a means of "soft war." Solutions may also not come to that, yet accountability is still a vast subject of discussion since there is a lack of reference to it regarding cyberwarfare. Investigating violators of the law on both an

international and domestic level is also heavily required in order to bring justice to perpetrators. However, management will not be well-organized without effective means of carrying out these investigations.

With everything to take in and evaluate, it is essential that the following solutions that end up in the resolution follow according to the stance your nation takes. Otherwise, your participation is void of the steadfast commitment of a great delegate. All this report does is state the facts and provide you with information. How you present your country is all you. Good luck!

Bibliography

Robinson, Michael, et al. "Cyber Warfare: Issues and Challenges." *Computers & Security*, vol. 49, Elsevier BV, Mar. 2015, pp. 70–94. *Crossref*, https://doi.org/10.1016/j.cose.2014.11.007.

NATO. "Cyberwar - Does It Exist? (NATO Review)." *YouTube*, 24 June 2013, www.youtube.com/watch?v=OuZpqlCI1Wo&t=1s.

Geers, Kenneth. *Strategic Cyber Security*. Kenneth Geers, 2011, books.google.ie/books?id=4h6KIDAfGhAC&pg=PA2&dq=978-9949-9040-7-5&hl=&cd=1&source=gbs_api.

"Cyberterrorism." *Wikipedia*, 20 Nov. 2023, en.wikipedia.org/wiki/Cyberterrorism.

"Moonlight Maze." *Wikipedia*, 31 Mar. 2023, en.wikipedia.org/wiki/Moonlight_Maze.

"Titan Rain." *Wikipedia*, 2 Nov. 2023, en.wikipedia.org/wiki/Titan_Rain.

"Operation Olympic Games." *Wikipedia*, 6 Oct. 2023, en.wikipedia.org/wiki/Operation_Olympic_Games.

"Stuxnet." *Wikipedia*, 21 Nov. 2023, en.wikipedia.org/wiki/Stuxnet.

"Duqu." *Wikipedia*, 29 Oct. 2023, en.wikipedia.org/wiki/Duqu.

"Flame (Malware)." *Wikipedia*, 29 Oct. 2023, en.wikipedia.org/wiki/Flame_(malware).

"2007 Cyberattacks on Estonia." *Wikipedia*, 18 Jun. 2023, en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia.

"Petya (Malware Family)." *Wikipedia*, 21 Nov. 2023, en.wikipedia.org/wiki/Petya_(malware_family).

"Operation Aurora." *Wikipedia*, 10 Aug. 2023, en.wikipedia.org/wiki/Operation_Aurora.

Zetter, Kim. “SolarWinds: The Untold Story of the Boldest Supply-Chain Hack.” *WIRED*, 2 May 2023, www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever.

“SolarWinds.” *Wikipedia*, 1 Nov. 2023, en.wikipedia.org/wiki/SolarWinds#2019%E2%80%932020_supply_chain_attacks.

"Cyberwarfare in the United States." *Wikipedia*, 27 May 2023, en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States.

“Cyberwarfare by Russia.” *Wikipedia*, 18 May 2023, en.wikipedia.org/wiki/Cyberwarfare_by_Russia.

Strategy for Operating in Cyberspace. U.S. Department of Defense, July 2011, csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Connell, Michael, and Sarah Vogier. *Russia’s Approach to Cyberwarfare*. Center for Naval Analyses, 24 Mar. 2017, www.cna.org/archive/CNA_Files/pdf/dop-2016-u-014231-1rev.pdf.

Hakala, Janne, and Jazlyn Melnychuk. *Russia’s Strategy in Cyberspace*. Directed by Sanda Svetoka, The NATO Strategic Communications Centre of Excellence, June 2021, stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

Medina, Eden. *Cybernetic Revolutionaries*. MIT Press, 2014.

Kaplan, Fred. *Dark Territory*. Simon and Schuster, 2016.

Singer, Peter W., and Allan Friedman. *Cybersecurity*. Oxford UP, 2014.

Orr, Trystan. “A Brief History of Cyberwarfare.” *GRA Quantum*, 1 Nov. 2018, graquantum.com/a-brief-history-of-cyberwarfare.

“Cybersecurity History: Hacking and Data Breaches.” *Monroe College*, www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches#:~:text=Cybersecurity%20history%20is%20interesting%20indeed,would%20become%20%E2%80%9Cthe%20internet.%E2%80%9D.

Jordan, Tim. *Cyberpower*. Routledge, 2002.

Kramer, Franklin D., et al. *Cyberpower and National Security*. Potomac Books, Inc., 2009.

Zhang, Li. "A Chinese Perspective on Cyber War." *International Review of the Red Cross*, vol. 94, no. 886, Cambridge UP (CUP), June 2012, pp. 801–07. *Crossref*, https://doi.org/10.1017/s1816383112000823.

"China Cyber Threat Overview and Advisories | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china.

"Lazarus Group." *Wikipedia*, 26 Nov. 2023, en.wikipedia.org/wiki/Lazarus_Group.

"How Did Barely Connected North Korea Become a Hacking Superpower?" *South China Morning Post*, 2 Feb. 2018, www.scmp.com/news/world/article/2131470/north-korea-barely-wired-so-how-did-it-become-global-hacking-power.

"Guidance on the North Korean Cyber Threat | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 23 June 2020, www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a.

"North Korea Cyber Threat Overview and Advisories | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea.

"South Korea." *Wikipedia*. 25 Nov. 2023, en.wikipedia.org/wiki/South_Korea#Cyber_security.

"Cyberwarfare and Iran." *Wikipedia*, 14 Nov. 2023, en.wikipedia.org/wiki/Cyberwarfare_and_Iran.

"Iran Cyber Threat Overview and Advisories | CISA." *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/iran.

"Unit 8200." *Wikipedia*. 17 Nov. 2023, en.wikipedia.org/wiki/Unit_8200.

"Tallinn Manual." *Wikipedia*, Wikimedia Foundation, 23 Nov. 2022, en.wikipedia.org/wiki/Tallinn_Manual.

CCD COE - the Tallinn Manual. web.archive.org/web/20130424162717/http://ccdcoe.org/249.html.

Group of Governmental Experts – UNODA. disarmament.unoda.org/group-of-governmental-experts.

Basu, Arindrajit, et al. "The UN Struggles to Make Progress on Securing Cyberspace." *Carnegie Endowment for International Peace*, 19 May 2021, carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491#:~:text=In%202004%2C%20the%20UN%20established,by%20a%20U.S.%2Dsponsored%20resolution.