BACKGROUND GUIDE

WAMUNC XXIV

Disarmament and International Security Committee

Letter From The Chair

Hi Everyone!

Welcome to WAMUNC 2022! My name is Anmol Chowdhary, and I am the chair of the Disarmament and International Security Committee this year. I am a freshman at The George Washington University, studying International Affairs with a potential concentration in security policy. I am originally from Glastonbury, CT, and I have been doing Model UN since middle school. I have attended a variety of conferences, including WAMUNC, so I am very excited to serve as a chair this year!

In this committee, we will be discussing the topics of cybercrime and cyber ethics, and cybersecurity within globalization. When choosing the topics for this committee, I really wanted to make sure that the topics were relevant to society today. Technology, now more than ever, has such a profound role in our lives, so it is crucial to discuss and determine potential solutions for the topics at hand. With evolving technology and capabilities, the security of the global community is at much greater risk. Keeping this in mind, in this committee, Topic A will be cybercrime and cyber ethics, in which we will greatly focus on the motives of hackers, the implications of cyber attacks, and the impact of cyber attacks on humanity. Whereas, Topic B will be Cybersecurity and Globalization. For Topic B, I am hoping for discussion focused more on strengthening security for the digital economy and global supply chains, keeping in mind the interconnected nature of the world and cyber attacks.

Outside of chairing WAMUNC, I am on the GW Model UN team and in the International Affairs Society. I am hoping to go to law school after college, so I also write for a legal journal on campus called the Justice Journal! In my free time, I also love playing golf and exploring DC!

Whether this is your first conference or your last, I am excited to have a weekend full of debate and discussion about these topics. I am looking forward to hearing all of your unique solutions and perspectives!

I am excited to see all of you in March, so happy researching and always feel free to reach out with any questions!

Best,
Anmol Chowdhary

COMMITTEE OVERVIEW

The Disarmament and International Security Committee was formed to address "disarmament, global challenges and threats to peace that affect the international community" ("Disarmament and International Security"). The scope of this committee has changed over years; however, the purpose always remains to protect the globe.

Currently, one of the greatest threats to international security is the misuse of advanced technology. In 2017, the United Nations Resolution 2341, the Security Council aimed to begin addressing the challenges that come with technology. This resolution asks nations to be more transparent regarding their technological practices, "to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks" ("Misuse of Information"). In fact, the UN Office of Counter-Terrorism, UNOCT, has developed protocols that have helped strengthen countries' responses to cyber terrorist attacks. For instance, the Cybersecurity and New Technologies programme attempts to strengthen the abilities of states in counteracting cyber attacks ("Misuse of Information").

In addition to this program, the Global Programme on Cybercrime specifically has objectives that focus on strengthening the overall response to this issue. The program specifically focuses on the geographic regions of Central America, Eastern Africa, the Middle East, North Africa, and SouthEast Asia and the Pacific. The Global Programme focuses on increasing investigation and consequences in procedures, establishing long-term effective protocols, and ensuring increased communication and transparency among the government and the public ("Global Programme").

There are many different types of cybersecurity threats. A cybersecurity threat is defined as, “any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information” (“7 Types”). Some examples of threats may include malware, emotet, and denial of service. Malware is often targeted towards the public as its most common form is through corrupt links, attachments, or files, which leads to software or systems becoming damaged. Whereas, an emotet, a type of malware, is defined by the Cybersecurity and Infrastructure Security Agency as, “an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. Emotet continues to be among the most costly and destructive malware” (“Emotet Malware”). Finally, denial of service (DoS), causes a computer system to be completely unresponsive (“7 Types”). Ultimately, all of these cybersecurity threats are dangerous to the public. Although the advancement of technology has many benefits, the drawbacks must be addressed effectively to protect the security of the international community.

Examples of Cybersecurity Attacks

Cybersecurity attacks are unfortunately quite visible in the international community. Some examples of cybersecurity threats include breaches with the 2016 election in the United States, SolarWinds, and the Colonial Pipeline.

Most notably, in 2016, it is said that Russia meddled with the United States’ election through hacking databases, attacking Hillary Clinton’s campaign, and the Democratic Congressional Campaign Committee and the Democratic National Committee. In addition, there was a great amount of misinformation propaganda spread throughout social media platforms. These actions directly impacted the election system upheld by the United States government (Abrams). According to the U.S. intelligence community, the objective of these attacks from Russia was to support Donald Trump’s campaign and provoke “distrust in American democracy” (Abrams).

Similarly, it is said that Russian intelligence was also behind a computer breach that released classified information about the United States government and companies in 2020. The hackers attached their malware to a commonly used software, SolarWinds, in order to reach a wide audience. It is estimated that this attack reached 18,000 SolarWinds customers, and infiltrated a variety of departments in the United States government such as the Commerce Department, the Department of Homeland Security, the Pentagon, the Treasury Department, and the U.S. Postal Service and the National Institutes of Health (Chappell, Bill, et al). Cyber attacks happen across the globe and represent a new manner of warfare.

Another instance of a cybersecurity threat can be seen with the Colonial Pipeline, the largest fuel pipeline in the United States. In this case, hackers were able to attack the networks of the Colonial Pipeline through the use of a compromised password. To gain control over the system again, the Colonial Pipeline company had to pay a ransom of $4.4 million to a Russian affiliated hacking group, DarkSide (Turton and Mehrotra). This case brings about questions regarding when it is appropriate to pay a ransom and even the role of the government in situations involving private companies such as the Colonial Pipeline.

BACKGROUND GUIDE

Topic A: Cybercrime and Cyber Ethics

Within cybersecurity, cybercrime and cyber ethics are important areas to consider. There are many different types of cyber crimes such as phishing scams, website spoofing, malware, ransomware, and fraud (“Top 5”). Phishing scams often take the form of innocent links or messages; however, they have the potential to steal an individual’s personal information. Similarly, website spoofing relies on an individual’s lack of awareness and causes individuals to open unreal websites. Once the website is opened, the hacker has access to the user’s system and personal data. Oftentimes, this form is supplemented with the crime of malware. Malware is a, “malicious software” that is “designed to gain access to or damage a computer, usually without the knowledge of the owner” (“What is Malware”). There are also different types of malware ranging from viruses that take over a system to trojans that release more malware into the system to even ransomware. Ransomware is a crime in which a hacker steals private data from an individual or company, and then demands money or payment from the target in exchange for the data (“Top 5”). In fact, according to McAfee, ransomware increased by 118% in the first quarter of 2019 (“McAfee Labs”). Finally, a common cybersecurity threat includes fraud crimes. There are several types of fraud, but the major two being email and internet fraud, and identity fraud. Email and internet fraud can often be conducted through phishing scams. However, identity fraud relies on a hacker stealing and using an individual’s personal information for their own personal benefit. This personal information includes an individual’s financial information and data. Oftentimes, after this information is stolen, hackers will sell the financial information and data to external parties (“Tips on How”). Cyber crimes can vary in extremity, but nevertheless they should all be taken seriously.

When evaluating cyber crimes, it is also important to consider the broader objectives of hackers. Most cyber crimes either aim to attack a specific target through viruses and malware or aim to corrupt computer systems through viruses and malware with the intention of manipulating or stealing data (“Tips on How”). These objectives can be met through cyber extortion, cryptojacking, and cyber espionage. Cyber extortion occurs when a hacker first takes control of a system and then begins “demanding money to prevent a threatened attack” (“Tips on How”). Cryptojacking is used when, “a criminal secretly uses a victim’s computing power to generate cryptocurrency” (“Cryptojacking”). Thus, through cryptojacking, a victim’s computer or system’s power is taken and used by a hacker, without the victim’s consent. Finally, cyber espionage occurs when, “hackers access government or company data” (“Tips on How”). Cyber criminals often attempt to obtain classified information for economic or political gains ("What Is Cyber Espionage?”). Cyber crimes can be very dangerous for the target as they lose access to their own data and systems. Especially in the case of classified information, hackers often re-sell this data or release the data to the public.

Cyber espionage is especially a crime of interest and can be demonstrated through the cases of Moonlight Maze and Operation Aurora. In 1998, the first and longest case of coordinated cyber attacks operated and resulted in, “thousands of stolen documents containing confidential information about American military technologies” (Paganini, 2017). This attack, Moonlight Maze, was the first of this large of a scale, and the malware, hackers utilized for this attack, is still used in society today (Paganini, 2017). These attacks cause the loss of confidential material, and specifically in this case, the loss of maps of military installations, troop configurations, and military hardware designs (Andress and Winterfeld). This case represents the danger of cyber espionage attacks to military operations and national security.

Similarly, in 2010, Google was attacked, leaving several Gmail accounts compromised. This attack is known as Operation Aurora. It is said that the hackers originated from China and specifically targeted accounts of Chinese human rights activists. Because of this incident, Google strengthened its procedures such as a hacking notification for users if their data was potentially compromised (“Operation Aurora”). Additionally, this was a unique case in that, Google decided to, “withdraw its Chinese operations from Beijing and instead serve the market from freer Hong Kong" ("Google Co-Founder"). This case represents the decisions companies make based on cyber espionage attacks and procedural changes in an attempt to strengthen their presence.

In order to protect their systems, nations have developed platforms to prevent cyber attacks and maintain the integrity of their information. Particularly, the United States Department of Defense has developed the Cybersecurity Maturity Model Certification (CMMC). The CMMC is, "a unified standard for implementing cybersecurity across the defense industrial base (DIB)" (Hill, 2021). This standard utilizes a variety of cybersecurity measures from mapping controls and processes to cyber hygiene to prevent future cyber attacks and limit damage from cyber attacks (Hill, 2021). In addition, in April of 2021, Spain's government announced their plan to invest more than €450 million in the coming years to strengthen the nation's cybersecurity sector (Hill, 2021). This investment will include promoting career positions in cybersecurity and developing Spain as "an international cybersecurity hub"(Hill, 2021). In addition to the new investment in cybersecurity measures, the Spanish government has also created an online Hacker Academy for Spanish residents to learn more about cybersecurity (Hill, 2021). Similarly, in May of 2021, Australia developed the Critical Infrastructure Uplift Program (CI-UP). This program aims to strengthen the cyber infrastructure of the country by determining weaknesses and vulnerabilities. CI-UP has developed mitigation strategies as well, in order to reach its aim to provide timely support in strengthening the crucial infrastructure of the country (Hill, 2021). Ultimately, some countries have begun to take action in strengthening their own systems to protect their data; however, protocols need to be established globally to eliminate cyber threats for all.

All nations do not have access to the same level of resources as others. Thus in order to combat cyber threats, it is crucial for nations to collaborate and develop international policies to move forward in the battle against cybercrime. In fact, when considering cybersecurity and the measures nations must take to protect themselves, the committee must consider the role of cyber ethics. Cyber ethics relates to the impact of the cyber world including cyber behavior and cybersecurity on humanity ("Cyber

Ethics”). With the increasing role of technology in the lives of all, developing policies relating to cyber ethics must be a priority.

There are a variety of problems pertaining to cyber ethics such as copyright and downloading files, crime and punishment, cyberbullying, and internet hacking. Issues such as copyright and downloading files, and crime and punishment directly relate to the expected behavior on the internet. Currently, governments have developed relatively strong policies relating to the consequences for disregarding copyright and downloading laws. Although they are seemingly innocent acts, the actions of children online often put them at risk when they aimlessly download files with their interest. Since they are so young, children are not aware of the consequences of copyright and downloading files. Thus, it is crucial to raise awareness for youth about the danger of the internet and how to avoid the risks with internet downloads. Similarly, since children spend so much time on the internet, there are risks associated with interactions online. Finally, internet hacking is a danger to the security of individuals. There needs to be a clear global standard set for the internet which includes consequences for hackers. The response to cyber attacks must be strengthened globally (“Cyber Ethics”). In addition to these aspects of cyber ethics, the global community must establish a policy that discusses internet censorship. Free speech and censorship are areas with many discrepancies.In addition to these aspects of cyber ethics, the global community must establish a policy that discusses internet censorship. Free speech and censorship are areas with many discrepancies. In fact, from 2006 to 2010, the Google search engine in China was, “run from within China and subject to self-censorship” (“Computer & Information”). However, this engine ended when Google’s operation in China changed due to Operation Aurora (Sheehan, 2018). Similarly, in 2009, the Ministry of Industry and Information Technology (MIIT) of the People’s Republic of China, announced their future plans to require the Green Dam Youth Escort software on all computers. Although this software was not officially established, it would essentially have the ability to filter material and censor the information individuals would have access to ("The Green Dam”). The international community must develop policies to maintain the rights of individuals and prohibit future policies restricting the public’s use of the internet. Ultimately, it is crucial to develop the internet as a safe space for all through creating policies that protect the rights of all.

To counter cyber attacks and strengthen cyber ethics regulations, some nations have developed cyber laws to ensure the prosperity of the internet in a safe manner. Cyber law is a relatively new area of law, so it is always changing and improving to protect the international community. However, there has been some progress. For example, the Indian government created the Technology Act in 2000, which aimed to, "improve transmission of data over the internet" ("Cyber Law"). In addition to this law, the United States has also developed several laws such as the National Cybersecurity Protection Act (NCPA). The NCPA created updated legislation regarding the policies for "information sharing between the private sector and the government" ("Cyber Law").

Possible Solutions

Policies regarding cyber crimes and cyber ethics must be developed globally to ensure the prosperity of all countries. Nations must develop international frameworks for the global community to follow that include both preventative and responsive measures. Oftentimes, systems are not up to date with privacy and security settings that leave systems more susceptible to cyber attacks. Thus, there needs to be an initial screening protocol developed, as well as steps to follow if a cyber attack does occur ("Cyber Law"). A key aspect for addressing cybercrime and cyber ethics is through spreading awareness and education. It is especially important to educate the youth about cyber attacks and for more information to be available about the dangers of cyber attacks ("Cyber Ethics"). Cyber attacks can pose a great risk to individuals; thus, it is important to create effective and feasible policies that are applicable to all states.

Topic B: Cybersecurity and Globalization

Globalization has become an integral part of the global community. Globalization is the, “spread of products, technology, information, and jobs across national borders and cultures,” through the, “interdependence of nations around the globe fostered through free trade” (Fernando, 2022).

This phenomenon shows “how trade and technology have made the world into a more connected and interdependent place”("Globalization"). However, globalization is quite complex with many positive and negative aspects. Some of the positive aspects of globalization include free trade, increased global economic growth, and an influx of shared information (Collins). Additionally, one major positive aspect of globalization is the technological advances and connections being made. In fact, technological advances caused the digital revolution in which economies in the world became more reliant on one another ("Globalization"). This is a strong benefit especially in creating increased cooperation between developed and developing countries. Because of globalization, developing countries were able to gain new technology and opportunities to support their economies with the help of developed countries. However, on the other hand, there are a few disadvantages to globalization. There is the transfer of disease, which is visible through COVID-19 and can also be seen with Ebola. Another disadvantage is that the transfer and sharing of technology has caused increased danger to intellectual theft and the security of the platforms initially created (Collins). Most importantly, a strong argument against globalization is that it has “made the rich richer while making the non-rich poorer” (Collins). Cybersecurity has a unique role with globalization in determining ways to establish equity with the development and trade of new technologies. Globalization has many positive impacts; however, there are also clear downsides, such as the unequal benefit and distribution of goods and services.

Because of the increasing interconnectedness of the global system, it has also led to greater connected technological threats. One example of a consequence of globalization connected to cybersecurity can be seen with the “WannaCry” cyber threat. In 2017, a phishing scam that used malware to corrupt systems attacked over 200,000 computers in 150 countries such as the United States, Russia, and Britain (Wallace). Because of the nature of this attack, hospitals and doctors’ offices were impacted and the healthcare system was damaged. Attacks of this nature and scale have the ability to impact all of society nationally, and internationally due to globalization. As many businesses and firms have sites located internationally, data sharing and communication must be monitored closely as a cyber threat can cause severe damage in present day society (Wallace).

With technological advancement, economic development has also been integrated into the digital world. The Global Ecommerce Association estimated that in 2020, 1 billion consumers would make purchases in other countries online (Ramachandran, 2019). With this many individuals interacting on the internet, it is important to maintain security of data and private information. However, according to McAfee, “Cybercrime now costs the world almost $600 billion, or 0.8 percent of the global GDP” (“McAfee Labs”). The global economy needs further infrastructure developed to establish greater security for consumers and businesses.

Cybersecurity even has a role in the international supply chains. Because of digital platforms, a hacker has the ability to corrupt supply chains. Disruptions to the supply chains can be made from other countries, but also from non-state actors such as ISIS. Any disturbance to the supply chain causes a negative impact for all countries involved, so it is especially important to maintain security over these platforms ("Globalization and the Cyber World”). The Colonial Pipeline is also an example of the impact a cyberattack can have on a supply chain. This pipeline is the provider for 45% of the fuel to the East Coast of the United States, so an attack would be very costly for both the pipeline and the recipients. Similarly, the SolarWinds breach represents that a single corrupted software update can impact a great number of users due to the interconnected nature of the company’s ecosystem. Especially due to the COVID-19 pandemic, hybrid work models and increased data online, there is more potential for attacks and cybersecurity risks within a company and ecosystem (Moss et al. 2021).

The digital economy is constantly changing due to new and advancing technologies. There need to be strengthened protocols and policies emplaced to ensure security. The Convention on Cybercrime 2001, the Budapest Convention, has general frameworks established but it needs to be improved and changed based on current technological developments. There needs to be better regulations and rules established that will define cybersecurity's role in globalization along with a legal framework for international violations (Lynch). Cybersecurity has a clear role in globalization, and it needs to be further recognized in order to achieve global security.

Potential Solutions

Cybersecurity is a newer component of globalization, but effective policies must be created to protect the international community. First, the committee must address the factors that were not conveyed in the Budapest Convention. This convention is outdated and must be advanced to strengthen cybersecurity procedures for global supply chains. Additionally, it is crucial to develop universal cybersecurity standards to ensure that all areas in the globe are following the safe rules and regulations (Lynch). Cyber norms must be developed to ensure a secure and safe digital ecosystem for all (Ramachandran, 2019). As this is a global effort, all countries must be involved. Thus, there needs to be an international framework created that will create detective and deterrence strategies (Ramachandran, 2019). In addition to strengthening existing systems, it is just as important to aid countries that do not have the same level of technological advancements to develop their systems with secure frameworks from the beginning. Developing countries must be equipped with strong technology; thus, all nations should promote collaboration and transparency within the international community (Guermazi, 2021). As mentioned earlier, globalization can have a positive impact and drawbacks, so it is important to determine how to minimize the drawbacks in a digital environment for both developed and developing nations.

Bloc Positions :

Bloc groups can be framed in multiple ways. In committee, I am hoping to see collaboration amongst all countries. However, this bloc group framework will help determine where different countries may fit in terms of policies established and level of development.

- Developed Bloc - countries who have a developed economy, developed infrastructure with cybersecurity
- Developing Bloc - countries who have a developing economy, little development of cyber platforms or cybersecurity
- Countries who are supportive of globalization
- Countries who are less supportive of globalization

Questions to Consider :

1. What differences exist in cybersecurity protocols between developed and developing countries and how can the gap be closed?
2. What legislation and policies has your country developed regarding cybersecurity? Can this framework be applied to the international community?
3. How can developing countries become more developed in terms of technology while maintaining security?
4. How can the digital economy be better secured?
5. What is the role of hackers and what are their motives?
6. To what extent can countries implement constraints on the way technology is used in their country?