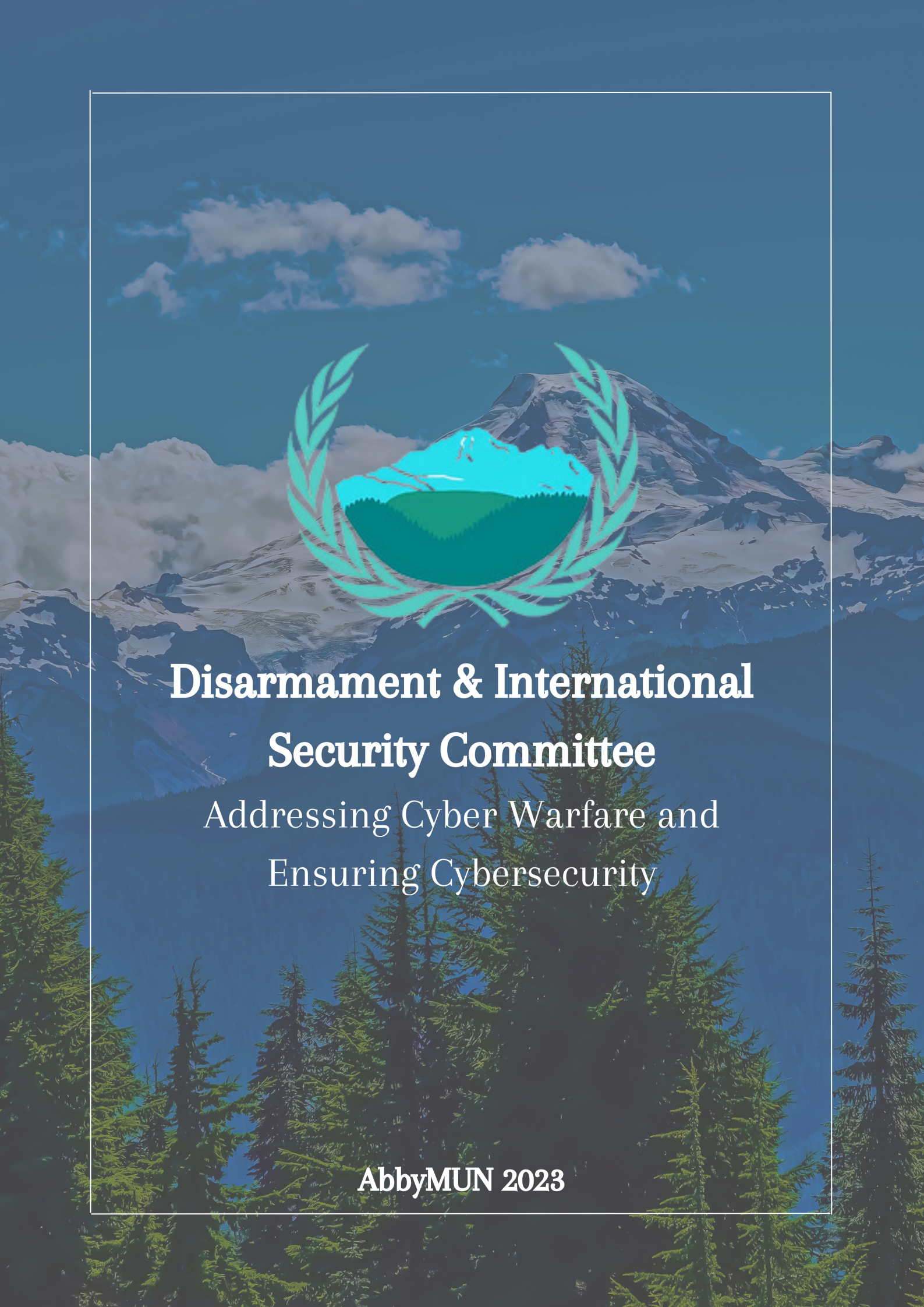


Disarmament & International Security Committee

Addressing Cyber Warfare and Ensuring Cybersecurity

AbbyMUN 2023

PRIME MINISTER · PREMIER MINISTRE

November 25, 2023

Dear Friends:

I am pleased to extend my warmest greetings to everyone taking part in the 2023 Abbotsford Model United Nations Conference.

This conference offers delegates a wonderful opportunity to experience international diplomacy firsthand and to gain deeper insights into pressing issues facing the world today. Through their research and preparation, students will learn more about the policies and positions of different countries on a wide variety of topics as they engage in debates and discussions with their peers.

I would like to thank the organizers for putting together a stimulating and rewarding program for everyone involved. I would also like to commend the students taking part for their hard work in preparing for these deliberations. I am certain that you will benefit greatly from this opportunity to lead, negotiate and collaborate, and that you will come away inspired to create positive change as informed and engaged global citizens.

Please accept my best wishes for a memorable and rewarding experience.

Sincerely,

The Rt. Hon. Justin P. J. Trudeau, P.C., M.P.
Prime Minister of Canada

Table of Contents

Director's Letter

Dear Delegates,

Before anything else, allow me to extend the warmest of regards to all of you delegates participating in the Disarmament and International Security Committee (DISEC). My name is Gurarmaan and I will be your Director for this Committee. I am currently in Grade 12 and enrolled in Abbotsford Senior Secondary, the host school for ABBYMUN. Alongside me are Haya, our Assistant Director, and Aaron, our Chair. Both of these highly capable staff members have contributed to this backgrounder just as I have, and are equally as thrilled to meet you all on the day of the conference.

I started my Model UN journey in my freshman year of high school. To be honest, as many young teenagers are, I was quite cynical about our world leaders at the time and channeled this cynicism into frequent complaints about the efficiency of the United Nations and global cooperation in general. Indeed, my initial intention upon joining the club was simply to criticize, rather than make any meaningful contributions. A good analogy would be to listen to the latest album of an artist that you despise for the sole purpose of disparaging them online (as a devoted fan of K-pop, I am all too familiar with this practice). However, my years of learning more and more about the United Nations have shaped my perspective. on international cooperation. It is, quite frankly, astonishing what the United Nations seeks to accomplish. In a world with vastly different political systems ranging from democracies to dictatorships, even being able to unite nations into a single organization is a big ask. And so, the fact that the UN can establish common ground between these countries, and even succeed in facilitating the pooling of their wealth for mutual aims should be applauded even by the UN's harshest critics. This is why I believe that Model UN is so valuable to students – it instills a recognition of the significance of global cooperation in this day and age. And while this may be my last year involved in Model UN before I graduate, there is no doubt in my mind that the torch will be carried on by the next generation of passionate MUNers.

Feel free to email me with any questions at DISEC.ABBYMUN@gmail.com

Looking forward to our meeting,
Gurarmaan Dhillon
Director of DISEC – ABBYMUN 2023

Committee Description

The Disarmament and International Security committee (DISEC) is also known as the First Committee (of the UNGA), which was founded in 1945. The committee plays a crucial role in dealing with disarmament, worldly challenges, and threats to international peace; by drafting solutions to such challenges based on uplifting the standards of international security. The First Committee is devoted to the connection and cooperation of its members, to maintain security—including matters surrounding the regulation of armaments and guiding demilitarization. However, the matters this committee pursues must be within the limits of the UN Charter, and provide recommendations to its Member States or to the Security Council. Furthermore, this committee collaborates with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament.

Earlier actions of the Disarmament and International Security committee include providing a recommendation/draft resolution surrounding the discovery of atomic energy; in which the General Assembly adopted, titled, “Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy” (1946). In recent years, DISEC has reviewed a multitude of draft resolutions on weapons of mass destruction and nuclear disarmament. In the committee's 76th session (2021), DISEC constructed an agreement on addressing information/telecommunications related to protecting and uplifting international security. One of the drafts approved was China’s “Promoting International Cooperation on Peaceful Uses in the Context of International Security”. This provision urged all Member States to produce strict procedures to promote global cooperation in materials, equipment and technology. In October of 2022, further draft resolutions (recommendations) were approved, including one majorly considering Nuclear Disarmament. Despite extensive opposition and concerns, the committee found grounds to place the environment of global security at the highest of importance. The following December, such recommendations were adopted by the General Assembly. Such recommendations relate to the global security threats in Ukraine, and the increased use of Nuclear weapons (highest since the cold war). Thus, the First Committee’s work allowed the assembly to speak to all states to pursue efforts in the disarmament of nuclear weapons (prominently to nuclear-weapon states), and to create measures to assess/prevent risks of miscommunication and miscalculation.

DISEC proves itself to be an essential committee in protecting international security, and prioritizing disarmament around the globe.

Topic Overview

As individuals, businesses, and governments grow dependent on new technologies, it has

increased concerns over international cyber security. The digitalization of storing information and data is also reliant on proper security measures and privacy; to minimize threats and improper uses of such information. Exploiting the cyberspace (technological/online world) is evident in operations outside of arm conflicts, but in them as well. The malicious usage of cyberspace possesses real risk to civilians, civilian infrastructure, and civilian data; and as the years go by, the risk on an international level increases. Furthermore, some states are creating military cyber capabilities, however, the use of cyber tools (purposely or accidentally) may cause diverse challenges on civilian infrastructures. Such civilian infrastructures include industries in telecommunications, transport, governmental, financial and even medical systems. There is overall increased potential for conflict/ability of State/Non-States to pursue attacks over international borders. In October of 2021, the Security Council held its first open-debate on uplifting peace and security in the cyber world. Such involvement may further develop measures to ensure security and peace. However, most threats in cyber security are often outside of actual armed conflicts. This is shown as malware is easily accessible to spreading around the globe to affect essential services. In spite of this, the International Court of Justice (ICJ) formed rules to forbid targeting civilians/objects, the use of weapons/attacks, and threats to medical services (protected under an international humanitarian law).

The Open-Ended Working Group and Group of Governmental Experts (created under the UN) stressed the need for a framework for State behavior relating to information and communications in technology; and prioritizing that cyberspace must never be a playing ground for military use in national or international conflict. The use of artificial intelligence is another concern through cyber security, with improper regulations and its rapidly growing discovery around the globe.

Overall, this dependence on digital technologies offers individuals and governments with new unpredictable vulnerabilities. It is difficult to address and tackle cyber security as state cooperation is minimal on protecting cyber security and fostering international peace. With such challenges, nations are often isolated to identify cyber attacks, and need to find flaws in an already weak system. In light of this instability of cyber security and cyber warfare, the Disarmament and the International Security committee is continuing in the provision of recommendations for states to work towards demilitarizing cyberspace and approving reinforced policies on cybersecurity.

12 DISEC
:A Timeline of Cyber History

The invention of the first modern computer, the ENIAC

The Electronic Numerical Integrator and Computer marked the beginning of the digital era, laying the groundwork for future advancements in computing and setting the stage for the cyber landscape we see today.

The rise of ARPANET

ARPANET, the precursor to the internet, fundamentally changed global communication and laid the foundation for the interconnected digital world, while also introducing new vulnerabilities to cyber attacks and threats to national security.

The Morris Worm

One of the earliest recorded instances of malware, raised awareness about the potential dangers of cyber threats and highlighted the need for robust cybersecurity measures to protect digital infrastructure.

The establishment of the UNGGE

The establishment of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security marked a critical step in recognizing the importance of international cooperation in addressing cyber warfare and ensuring global cyber security.

The cyber attacks on Estonia

The atacks targeted government institutions, banks, and media outlets, underscored the potential for cyber warfare to disrupt the functioning of a modern state, prompting international discussions on the need for stronger cybersecurity protocols and defense mechanisms.

The Stuxnet Worm

A sophisticated cyber weapon that targeted Iran's nuclear program, highlighted the potential for nation-states to use cyber weapons as a means of strategic warfare, leading to heightened concerns about the implications of cyber warfare on international security and stability.

Edward Snowden's revelations about the scope of the NSA

The National Security Agency's global surveillance programs sparked debates about the balance between national security and individual privacy, resulting in increased scrutiny of government surveillance practices and the need for enhanced transparency and accountability in cybersecurity policies.

The United Nations adopted the norm of responsible state behavior in cyberspace

This emphasized the importance of respecting international law and human rights in the context of cyber operations, and signaling a significant milestone in the development of international norms for addressing cyber warfare and ensuring global cyber security.

The WannaCry ransomware attack

This affected hundreds of thousands of computers worldwide, demonstrated the potential for cyber attacks to cause widespread disruptions and economic losses, highlighting the urgency for stronger collaboration between governments and the private sector to strengthen cyber resilience and response capabilities.

The GDPR's implementation of the General Data Protection Regulation

The European Union's implementation of the General Data Protection Regulation set a global precedent for data protection and privacy regulations, influencing the development of similar legislative frameworks worldwide and emphasizing the need for robust data protection measures to safeguard individuals' personal information in the digital age.

Source: History.com

The SolarWinds cyber attack

This attack compromised numerous U.S. government agencies and private organizations, exposed the vulnerabilities in global supply chains and underscored the importance of implementing stringent security measures to detect and prevent sophisticated cyber threats, prompting renewed efforts to enhance cyber defense capabilities and resilience.

The establishment of the CISA

The establishment of the Cybersecurity and Infrastructure Security Agency as a standalone entity within the U.S. Department of Homeland Security marked a significant step in strengthening the nation's cybersecurity posture and resilience, reflecting the increasing recognition of cybersecurity as a critical component of national security and the need for dedicated, coordinated efforts to address evolving cyber threats.

Historical Analysis

Cyber security has a deeply rich history on the global stage. The Morris Worm of 1988, being one of the earliest recorded cases of malware, was a wake-up call to the international stage of the dangers that malware posed to global security. It was written by student at Cornell University, exploiting several vulnerabilities of the systems that it targeted. The result was around 6 000 machines affected, each one often taking days to purge of the virus. With a total economic impact of up to $10 000 000, clearly something had to be done. Luckily, the United Nations was quick to respond, with the establishment of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

And while this move did send a message that the issue of cyber security need not be so bleak, it was not enough on its own. As time went on and computers saw more widespread use outside of scientific facilities, the threat of cyber attacks grew in similar proportion. The cyber attacks on Estonia in 2007 are a clear example of this, targeting government institutions, banks and media outlets alike. This was a major turning point for the threat of cyber attacks. Suddenly, it was not so abstract to the public that it only affected distant scientists – attacks on the very institutions that serve as the backbone of a modern state sent a clear message that cyber attacks could throw international security into jeopardy.

And while the world did see an increase in government action to correct this issue, there continues to be discussions surrounding the ethics of balancing state intervention and individual privacy.

Edward Snowden, a former employee of the United States' NSA, spearheaded these discussions in 2013, leaking highly classified information surrounding the agency's reach on the American public. For instance, the state could directly access Americans' Google and Yahoo accounts. They were also secretly paying telecommunications companies to access their networks, enabling the government to spy on virtually any phone conversation or internet activity that citizens assumed to be private.While much of the practices that Snowden detailed continue to be used, there remains a debate around the extent to which governments can sacrifice individual privacy for national security. Defenders of the NSA and similar organizations will make the argument that all these measures are for the "greater good", and that being spied on by a well-intentioned government should be preferred over being hacked by a criminal or enemy state. However, opponents will claim that such utilitarianism has no place in a liberal democracy. When the government tramples over the rights of its citizens, it is easy to go past the point of no return. All it takes is a single bad actor in a powerful position to make use of the allotted powers in an ill-intentioned manner. After all, part of preserving democratic states is ensuring that the government is subservient to its citizens, not the other way around.

And while these debates continue to be had, cyber attacks continue to be a significant issue, now merging with newer technologies like the blockchain. Most famously, "cryptojacking" is the act of exploiting a computer to mine cryptocurrencies like Bitcoin. This adds a new layer to the incentive structure for hackers – not only does the practice attract those with malicious intents, but it also attracts tech-savvy individuals looking for easy money. The result is affected devices having their processing power exploited to line the hackers' crypto wallets, slowing the devices down. These attacks often go unnoticed by victims, who simply view their computers slowing down as a sign of regular use, which is part of what makes cryptojacking so dangerous. And so if there's any takeaway from all these events, it is that cyber attacks are a complicated issue with no easy solution. Their evolving nature requires continued international intention, all while safeguarding individual privacy.

Current Situation

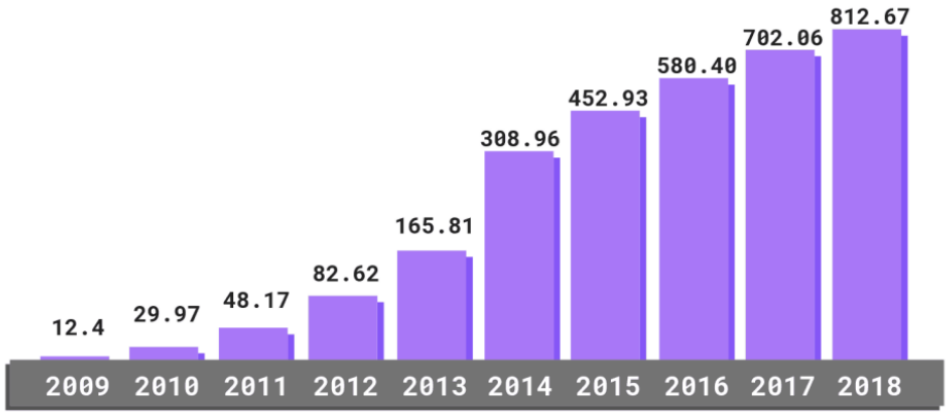
Before beginning, it is fundamental to have a thorough understanding of what cybersecurity is. Cybersecurity refers to the practice of protecting computer systems, networks, and data from digital attacks. It involves implementing various measures to safeguard information technology infrastructure from unauthorized access, data breaches, and other cyber threats. These measures include the use of strong security protocols, such as firewalls, antivirus software, and encryption, to prevent unauthorized access to sensitive information and to detect and mitigate potential

security breaches. Additionally, cybersecurity involves educating users about potential risks, promoting best practices for safe online behavior, and regularly updating systems to protect against evolving threats. Maintaining strong cybersecurity is essential in safeguarding the confidentiality, integrity, and availability of data, thereby ensuring the privacy and security of individuals, businesses, and organizations operating in the digital sphere.

Furthermore, cyber warfare is when countries or groups use computer attacks such as hacking or viruses to interfere with other countries' computer systems or steal important information. They do this to cause chaos, gain an edge over their rivals, or even to make money. Targets can include government websites, banks, or even power plants. It is a great challenge to deal with cyberthreats as it is hard to know who's behind them, and things online change all the time, making it tough to protect against.

As of 2023, addressing cyber warfare and ensuring cyber security remains challenging, with both state and non-state actors having to constantly adapt to exploiting vulnerabilities in digital systems. Governments and international organizations continue to try and keep up with the cyber threats, which have expanded in sophistication overtime, targeting critical infrastructure, financial institutions, and sensitive data.

The increasing reliance on technology along with the increase of interconnected devices in the Internet of Things (IoT) system has amplified the potential impact of cyber attacks. This is posing significant risks to national security, economic stability, and public safety. Consequently, there is a growing emphasis on promoting international cooperation and information sharing to fight these threats effectively, with efforts such as the United Nations' initiative to establish responsible state behavior in the cybersecurity world.



Total Malware Infection Growth Rate (In Millions)

The United Nations has been actively addressing the impact of cyber warfare on global security and stability, emphasizing the need for international cooperation and the development of norms to govern responsible behavior in cyberspace. Through various initiatives, the UN has facilitated discussions among member states, encouraging the establishment of guidelines that prioritize the protection of human rights and the rule of law in the context of cyber operations. Additionally, the UN has supported the creation of expert groups and committees to study the implications of cyber warfare and develop frameworks for addressing emerging challenges in the digital realm. By promoting collaboration among governments, private sectors, and other stakeholders, the UN has contributed to the establishment of partnerships and platforms for sharing best practices and enhancing cybersecurity capabilities worldwide.

Finances, too, are impacted from cyber warfare. Cyber warfare can make a catastrophic financial mess for both businesses and the whole economy. For companies, it means spending lots of money to fix things after an attack, like checking what went wrong, repairing systems, and making security stronger. They can also lose important data or ideas, which can make it hard for them to compete and might even lead to legal problems. When cyber attacks mess with things like power grids or money systems, it can make the whole country's economy shake. Governments also have to spend great financial figures to protect against these attacks and fix things when they go wrong.

Moreover, making use of new technologies -such as artificial intelligence- into cybersecurity frameworks shows capability in enhancing defense; but it also raises concerns about potential new vulnerabilities and ethical issues. Amidst these efforts, the economic faltering due to cyber attacks remain prominent, with businesses and governments bearing substantial financial losses from data breaches, ransomware attacks, and intellectual property theft, highlighting the importance of strong cybersecurity measures and risk management protocols.

Simultaneously, the environmental impact of cyber warfare is increasingly significant, as maintaining secure data centers and the carbon footprint associated with digital infrastructure underlines the need for proper cybersecurity practices and the usage of energy-efficient

technologies. Consequently, the current addressing of cyber warfare and ensuring cyber security integrates technological advancements, regulatory frameworks, and environmental consciousness to foster a more resilient and secure digital ecosystem globally.

Past Involvement

The United Nations has undoubtedly made progress in resolving the pressing issue of cyber attacks. As stated earlier, the establishment of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security was a great way for the United Nations to get their foot in the door leading to protect from cyber attacks. In addition, resolutions from the United Nations Security Council made in 2014 and 2017 call upon member states to take internationally cooperative action in their efforts to prevent terrorists from exploiting technology and communications for their means. However, the issue remains persistent, with problems ranging from economic to environmental ensuing from cyber attacks.

Among the United Nations' latest efforts to preserve international security in cyberspace is the adoption of the Global Counter Terrorism Programme on Cybersecurity and New Technologies in April 2020. This programme was and continues to be developed under the cooperation of various partners within the United Nations such as UNICRI and INTERPOL, and is funded by the European Union, Japan, the Republic of Korea, Saudi Arabia and the United Arab Emirates. Its main focus is on empowering member states to combat cyber attacks, providing them with the necessary resources to do so. Evidently, the programme has had a large impact. Since its inception, it has trained over 3300 officials from more than 150 member states in matters concerning preserving security within cyberspace. Of course, it has also stressed the importance of maintaining human rights in its efforts, incorporating surrounding discussions into its protocols. The results have been quite extensive thus far. The programme has extended assistance to Maldives, Bangladesh, Malaysia, Indonesia and the Philippines in enhancing the skills of officials in collecting open-source information online in their counter-terrorism efforts. Burkina Faso has been assisted by Germany in the development and use of new technology to protect critical infrastructure from terrorist attacks. The programme has also produced two reports on building knowledge on counter-terrorism in the context of a world rampant with artificial intelligence. With these efforts and many more, it is clear that cyber security has been given the international attention it deserves. And while these definitely do signal an international focus on the issue and have achieved concrete results, there are definitely some key limitations to the programme. For one, as outlined earlier, cyber attacks have continued to run rampant around the world and show no indication of stopping. This is not to say that the programme has been severely lacking in its performance, but rather a signal that there is room for improvement. In addition, its survival is reliant on the contributions of only a select few countries out of the many

member states part of the UN. It lacks the financial backing of enormous economies like those in America and China, and is thus limited in what it considers as feasible action.

That being said, other countries have not been completely absent from the necessary conversations surrounding the international community's role in cyber security. In October 2022, the United Nations Security Council Counter-Terrorism Committee (CTC) unanimously signed onto the Delhi Declaration, committing the member states to prevent and combat digital forms of terror. It outlined the various mediums through which digital terrorism takes form, like drones, social media and online terrorist financing. It also provided a set of guiding principles to assist member states in countering the use of certain technologies in terrorism, and outlined how states can use the said technologies to combat terrorism. And while at the end of the day, these principles are non-binding, the declaration was nonetheless a strong indicator that there is strong interest in the international community to prevent cyber attacks from becoming too widespread.

Bloc Positions

Bloc #1: USA, Canada, Australia, UK and Support States (For ensuring a secure and private cyberspace; whilst eliminating cyber threats to civilian infrastructure)

This bloc primarily consists of developed countries such as the United States of America, Canada, Australia and the United Kingdom. Main concerns over cybersecurity relate to ransomware attacks that target necessary civilian infrastructure, and the privacy and freedom of civilians. For example, Canada has previously committed $27 million to cyber capacity infrastructure projects and collaborations with organizations to market a secure and free cyberspace. Similarly, the 2023 USA National Cybersecurity Strategy also uplifts the protection of critical civilian infrastructure (outlined as hospitals and clean energy facilities). Furthermore, the USA's strategy aims to create a dependable/stable cyberspace— including prioritizing individual privacy, accountability for larger companies, and collaboration internationally. Overall, the strategy aims to relocate the responsibility of cybersecurity to organizations that have the actual resources to defend the online world. This bloc will aim to implement cyber security measures for civilians/infrastructure, protect international peace, and a free digital environment for users.

Bloc #2: Russia, China, Supports (For gaining control over their own cyberspace)

This second bloc is made up of countries like Russia, China and possible supporters (like Pakistan). The main initiative of this bloc is similar in the first Bloc with the USA to create stability in cyberspace, but to gain more control over their own internet. Russia believes in creating a cyberspace that is controlled by the government, and granted privileges to restrict

certain online content. This goal is supported in the Russian-sponsored UN Open-Ended Working Group (OEWG). This group currently outlines sovereignty and eradicates conflicts in political affairs in cyberspace. Compared to the Group of Governmental Experts (supported by the USA/Canada, GGE), the OEWG does not express the same openness and individuality for citizens in cyberspace. This is controversial for many states as in which consensus would promote an open/free online world, or one that has states controlling their cyberspace and choices. Repressive states, like China, also aim to gain control over their cyberspaces and the digital environment their civilians and businesses use on the daily. Primarily to narrow down views that do not align with the government's standards (including many authoritarian states).This goal may present itself with a large threat to international security as states are diverted from preventing border-crossing ransomware threats.

Bloc #3: Developing & Non-Aligned Countries

The third and final bloc consists of developing nations (Indonesia, Trinidad, Bangladesh, Thailand, etc.) that face challenges (financial, frameworks) in creating a secure cyberspace and are in favor of components in the OEWG and the GGE. It is necessary for countries in this bloc to prepare and prioritize building cyber capabilities— with collaboration of high-income/developed nations and also existing frameworks. However, this bloc stresses that members must take further initiative in preventing use of data and technology maliciously, and urges the need for international cooperation. Countries within this bloc may also find proper representation in matters related to cybersecurity and cyberwarfare— to gain diverse strategies that will cause long-term stability online, internationally.

Potential Solutions

As cyber attacks are such a multi-faceted issue, it is only natural that the solutions are similarly diverse. The most obvious answer is to form a new committee on combatting cyber attacks, with hopefully a larger membership than before. After all, the Global Counter Terrorism Programme on Cybersecurity and New Technologies did have significant achievements in spite of its somewhat limited participation. This committee could have various commitments. It could devote itself to research on the issue, releasing reports on the latest threats that cyber attackers pose and the methods by which they are realized. They can similarly provide information on the various methods a government can use to effectively utilize the cyberspace, all while maintaining its security in doing so. And while this likely has the largest impact to cost ratio, it still places a large burden on the member states to implement what the reports outline. Thus, a committee can supplement these reports with more material support for the member states that may not have the means of maintaining its security on its own. The support can range from a process of delivering grants to these states to sending officers to directly deliver the tools and knowledge necessary for

the states' cyber security. The latter would be similar to how the Global Counter Terrorism Programme on Cybersecurity and New Technologies was able to train thousands of officials on the subject. With greater participation, however, this hypothetical committee would hopefully be able to deliver on these goals to a much larger extent than before.

For delegates who desire a more creative solution than adding yet another committee to the United Nations, an alternative solution would be a body structured around a certain set of goals, like combating cyber terrorism. Member states would be required to contribute some percentage of their GDP in exchange for an organization similar to INTERPOL. It would be an international force dedicated to searching for and eliminating cyber terrorist groups. This may be preferred over simply using national law enforcement agencies, as cyber terrorists are often located in a different country than their victims. While the victims' law enforcement agencies may not be able to track down criminals abroad, an international force would have better luck in its ability to facilitate cooperation on eliminating cyber security threats.

Of course, any financial contribution to a United Nations group may be too much of an ask for the more isolationist states. Should the more expensive solutions outlined above fail to get sufficient support, an isolationist-friendly alternative does exist. One possible resolution is to simply require that member states dedicate a certain amount of their defense budget to their own cybersecurity programmes. A downside to this is that there will be no centralized authority keeping track of how efficiently the money is being spent, and the available knowledge on how to efficiently develop safeguards against cyber attacks will be limited to what existing United Nations efforts provide. However, member states would likely have a lot fewer reservations on voting for such a proposal, considering that they would be completely in control of how their money is spent. Of course, many more solutions exist, and we encourage delegates to stay creative in how they tackle resolutions, as opposed to using cookie-cutter solutions that can be found in any committee with a few key word changes. Let the above solutions simply serve as a springboard for the many creative ideas that will be presented in the conference.

Discussion Questions

1. How much should states contribute to a global cyber security effort, as opposed to domestic efforts?

2. At what point do the impediments to individual privacy hold greater weight than the benefits to cyber security?

3. Given the UN's past involvement, to what extent is there a need for further focus on the issue of cyber attacks?

4. Should DISEC impose punishments on countries that utilize cyber attacks in their war strategies?

5. To what extent are the countries with larger economies responsible for assisting smaller countries in their efforts to secure their cyberspace?

Further Resources

1. https://www.un.org/en/ga/first/

2. https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity

3. https://unsceb.org/topics/cybersecurity

4. https://www.cisco.com/c/en_ca/products/security/what-is-cybersecurity.html#~how-cyber security-works

5. https://www.imperva.com/learn/application-security/cyber-warfare/

Bibliography

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.

Bogost, Ian. "'Netwar' Could Be Even Worse Than Cyberwar." The Atlantic, 28 Feb. 2022, www.theatlantic.com/technology/archive/2022/02/russia-ukraine-conflict-cyberwar/622931/.
"China's Evolving Cybersecurity and Cyber Development Strategy." The National Bureau of

Asian Research (NBR), 10 Sept. 2018, www.nbr.org/publication/chinas-evolving-cybersecurity-and-cyber-development-strategy/.

"Cyber Operations During Armed Conflicts." International Committee of the Red Cross, 9 June 2023, www.icrc.org/en/document/cyber-warfare.

"Cybersecurity | United Nations." United Nations - CEB, unsceb.org/topics/cybersecurity.

"Delegates Propose New Programme of Action for Struggle Against Threats to Cybersecurity, in First Committee Thematic Debate." press.un.org/en/2021/gadis3673.doc.htm.

"Establishing Cybersecurity Norms in the United Nations: The Role of U.S.-Russia Divergence."

Harvard International Review, 26 Nov. 2021, hir.harvard.edu/establishing-cybersecurity-norms-in-the-united-nations-the-role-of-u-s-russia-divergence/.

"Everything You Need to Know About Cybersecurity in 2022." World Economic Forum, 18 Jan. 2022, www.weforum.org/agenda/2022/01/cyber-security-2022-global-outlook/.

"Everything You Need to Know About Cybersecurity in 2022." World Economic Forum, 18 Jan. 2022, www.weforum.org/agenda/2022/01/cyber-security-2022-global-outlook/.

"First Committee Approves 60 Texts, Rejects 1, with Delegates Differing over Weapons of Mass Destruction, As Action Phase Concludes." press.un.org/en/2021/gadis3678.doc.htm.

"First Committee Sends 20 Nuclear Weapons Drafts to General Assembly Requiring 33 Separate Votes for Adoption." press.un.org/en/2022/gadis3701.doc.htm.

"The First Ever Global Meeting on Cyber Norms Holds Promise, But Broader Challenges Remain." Council on Foreign Relations, 26 Sept. 2019, www.cfr.org/blog/first-global-meeting-cyber-norms?ref=hir.harvard.edu.

"UN General Assembly - First Committee - Disarmament and International Security." Welcome to the United Nations, www.un.org/en/ga/first/.

"Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?" Council on Foreign Relations, 18 Mar. 2021, www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

United Nations. "Cyberconflicts and National Security." United Nations, www.un.org/en/chronicle/article/cyberconflicts-and-national-security.

"Groups of Member States." United Nations, www.un.org/en/model-united-nations/groups-member-states.

The Washington Post, 28 June 2021, www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/.

What is cyber warfare: Types, examples & mitigation: Imperva. Learning Center. (2021, November 9). https://www.imperva.com/learn/application-security/cyber-warfare/
United Nations. (n.d.). Towards Cyberpeace: Managing cyberwar through international cooperation. United Nations.

https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

Cisco. (2023, March 14). What is cybersecurity?. Cisco.
https://www.cisco.com/c/en_ca/products/security/what-is-cybersecurity.html

Encyclopedia Britannica, inc. (2023, September 20). Cyberwar. Encyclopædia Britannica.
https://www.britannica.com/topic/cyberwar

TIM MAURER & ARTHUR NELSON. Carnegie's Cyber Policy Initiative. (n.d.). The global cyber threat to financial systems – IMF F&D. IMF.
https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

"Cryptojacking." Wikipedia, the Free Encyclopedia, Wikimedia Foundation, Inc, 1 Nov. 2023, en.wikipedia.org/wiki/Cryptojacking. Accessed 8 Nov. 2023.

"Cybersecurity and New Technologies." Welcome to the United Nations, www.un.org/counterterrorism/cct/programme-projects/cybersecurity.

"Edward Snowden." Wikipedia, the Free Encyclopedia, Wikimedia Foundation, Inc, 22 Oct. 2023, en.wikipedia.org/wiki/Edward_Snowden. Accessed 8 Nov. 2023.

"Morris Worm." Wikipedia, the Free Encyclopedia, Wikimedia Foundation, Inc, 26 June 2023, en.wikipedia.org/wiki/Morris_worm. Accessed 8 Nov. 2023.