CHARGER MUN

University of New Haven • Notre Dame High School

United Nations Security Council 2

As your Dais, we would like to extend to you a warm welcome to our Second Annual ChargerMUN Conference on Sunday, December 9th of 2018. As members of the University of New Haven Model United Nations Program, our aim is to use this conference as a way to transmit the experiences that we have had in similar, college-level conferences, and to encourage cooperation and participation as we learn more about the field of international relations and global politics in dealing with real-life world issues.

Your Dais is made up of your chair, Estefano Eichentopf Palazuelos, a junior year college student studying for a bachelor's degree in Economics and another bachelor's degree in International Diplomacy and Development. He has been a delegate in 4 award-winning National Model UN conferences with the University of New Haven. In addition, he was the head delegate of University of New Haven's Model UN team for the NMUN Conference in Washington DC in November of 2018. The Dais also includes your co-chair, Rebekah Sherer, a junior year college student studying for a bachelor's degree in Criminal Justice with a minor in Political Science. Rebekah is another veteran delegate of the University of New Haven's Model UN program and was part of the university's outstanding delegation in NY earlier this year. We hope that our experience will be beneficial and helpful so that you can understand the proceedings of the real UN, as well as the typical process of Model UN conferences.

The topic before the Security Council is:

Cybersecurity in the Digital Age

As a simulation of the proceedings at the United Nations, this conference will simulate the proceedings of the Security Council headquarters in New York City. As this is a single-day conference, the day will be split into 2 committee sessions and a short voting bloc session, with roll call taking place at the start of each session. Once in committee, time is split between formal session, where individual delegations are allowed to speak to the committee for brief periods; and informal session, which is split between moderated and unmoderated caucus. During Formal Session, delegations will individually address the committee as a whole. During Moderated Caucus, delegates will discuss a specific topic as proposed to the Dais. Finally, during Unmoderated Caucus, delegates will operate freely as they form working groups in hopes of creating a resolution, or a possible solution to help address the problem. We ask that you remain professional, energetic, and cooperative throughout this conference and ongoing debate.

We would like to remind all delegates that the most important part of the United Nations is inclusiveness and cooperation, and therefore we hope to see all members of the committee willing to hear the views of fellow Member States, while focusing on creating a solution as a group of equals to solve the world issues assigned to the committee. Please remember to remain in character and work to represent your country accurately while engaging in civil and diplomatic debate with other delegates.

CHARGER MUN
UNIVERSITY OF NEW HAVEN • NOTRE DAME HIGH SCHOOL

Committee Overview

The Security Council was established on October 24, 1945. The goal behind the creation of the Security Council is to maintain international peace and security. In order to maintain this goal, the Security Council oversees various global conflicts and threats to determine the necessary measures to solve the pressing issues within the international community. These measures can range from declarations and agreements to sanctions and peacekeeping operations.

The Security Council is comprised of 15 members, split into geographical groups to ensure representation from each region. These regions include Africa, Asia-Pacific, Eastern Europe, Latin America and the Caribbean, and Western Europe. Out of these 15 members, five are permanent members and ten are non-permanent members. The permanent members are China, France, the Russian Federation, the United Kingdom, and the United States. The General Assembly elects the non-permanent members for two-year terms. Currently, the non-permanent members are Bolivia, Ethiopia, Kazakhstan, the Netherlands, Sweden, Côte d'Ivoire, Equatorial Guinea, Kuwait, Peru, and Poland. In cases where the topic at hand effects an area or Member State that is not being represented within the Security Council, these non-participating Member States can join the discussion as observing members. Observing members can participate in a discussion and assist in the resolution making process, however, they cannot vote on substantive issues, such as voting to pass a draft resolution.

The Security Council's mandate states that it seeks to maintain international peace and security through the development of positive relationships with all nations and by working to solve international issues while advocating for human rights. Unlike other organs of the UN, the Security Council's decisions and resolutions are legally binding and executed immediately.

The main objective of the Security Council is to maintain international peace and security. One of its primary ways to achieve this goal is by monitoring and preventing different forms of warfare and conflict. With the rapid evolution of information communication technologies (ICTs), like the computer or cell phone, as well as the increased cybernetic storage and usage of information by both private and public groups and organizations, cyberspace has become a potential platform for confrontation between States and non-state agents. Non-state actors are defined as an individual or organization with significant political influence but not allied to any particular Member State. Due to the risk of a possible new age of cyber-warfare, it is vital that the UN Security Council work on bettering global standards in cybersecurity.

The Security Council does not meet on a consistent basis but instead gets called into session when matters of peace and security need to be addressed. Due to the seriousness of breaches of peace and security, the Security Council can choose at any point to pause discussion on one topic and move to discuss a topic that they feel is prioritized. This allows for "emergency agenda changes" in cases where a serious issue may require immediate discussion.

One of the biggest differences between the Security Council and the other committees is the role of the P5 Member States during the voting process. The P5 Member States have "veto power." Like the other committees, in order for a resolution to pass, a majority of the committee must vote yes. In the Security Council, however, even if there is a majority agreement on the document, if a P5 Member State votes "no" or "against," their "veto power" goes into effect and the document does not pass.

CHARGER MUN
UNIVERSITY OF NEW HAVEN • NOTRE DAME HIGH SCHOOL

Statement of the Problem

With the rapid advancement of technology over the past couple of decades and as the global threat of cyber-attacks and cyber warfare increases with the advent of easy access to ICTs, the global community has begun placing more emphasis on cyberspace security. Therefore, a strong approach towards ensuring cyber security is crucial, as more digital information is at risk of being appropriated by a wider audience than intended, threatening the stability and development of Member States.

Without a proper strategy on how to standardize international cybersecurity, all Member States stand to lose significant assets which are becoming increasingly accessible through modern ICTs. The consequences of cyber warfare targeting the information and assets of Member States are wide-reaching, spanning from private civilians to corporations, to governments, and even military organs worldwide. Cyberwarfare is defined as the method of using technology such as computers as a weapon. This risk comes not only from the possibility of cyber warfare between states but between states and non-state actors. The increasing availability and free access to ICTs have allowed non-state actors to grow as a threat through their use of the internet and mass communication platforms.

Due to the fast pace at which ICTs and other innovative technologies are being developed, adapted, and disseminated, cybersecurity and countermeasures against this threat must be adopted and implemented in a timely manner. This will prevent a new age of cyber warfare and cyber terrorism that would affect all facets of society.

History of the Issue

The first computer virus appeared in 1971 and became known as the Creeper Virus. As a response, the first antivirus, the Reaper, was created to delete it from the system. This marked the beginning of the history of cybercrime. After this attack, network security was under fire.

Cybersecurity was first brought up as an issue by the UN General Assembly (GA) in 1999, when they passed GA resolution 53/70, entitled "Developments in the Field of Information and Telecommunications in the Context of International Security." This resolution outlined the importance of "information security" and encouraged multilateral cooperation in identifying potential threats. From then on, the issues only escalated to become an international problem. To combat this, the UN released A/RES/57/239 which addressed the need for cybersecurity increases due to the influx of countries that participate in the information society.

It wasn't until 2001, with GA resolution 55/63 titled Combating the criminal misuse of information technologies, that the UN began to progress towards a definition of cybersecurity and measures to combat the misuse of ICTs. This resolution set forward frameworks for a legal response, prosecution, and cooperation between the Member States to act against the criminal use of ICTs, while promoting international development and the sharing of technology and data in an effort to combat misuse of ICTs.

Starting in 2007, the International Telecommunications Union (ITU) began to play an active role in the standardization of cybersecurity by introducing the Global Cybersecurity Agenda (GCA). This plan gave a framework for all Member States which consists of 5 main approaches: legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation.

According to a recent study by the UN Institute for Disarmament Research, more than 40 Member States have developed a form of military cyberspatialities. Out of these 40 Member States, twelve have developed forms of offensive cyber warfare. The most recently appointed group of government experts gathered for week-long sessions in New York and Geneva in August 2012, January 2013, and June 2013 to discuss these forms of cyberwarfare. This session went along with bilateral U.S negotiations with Russia and China on cybersecurity.

Current Situation

Recently, more attention and scrutiny has been placed on cybersecurity measures, as ICTs become a more accessible means for individuals and groups to act in illegal ways. The most recent example of such an occasion is the "Wannacry" ransomware attack that stretched around the globe in 2017. During this attack, information and data on infected computers were locked and ransoms were issued to the users, threatening the destruction of these files if a fee was not paid in time. The rapid spread of this attack displayed the need for protection within ICT tools and equipment, to make it harder to spread a cyber attack so efficiently.

At the same time, although there has been significant progress in the creation of legal frameworks to counter cyber attacks and the illegal use of ICTs, there is no established rapid response system that would allow law enforcement to isolate the source of these attacks. While many government agencies and authorities have employed their own operations, the pooling of resources and data, as well as the development of regional responses and monitoring programs could provide a more reliable framework for combatting cyber attacks and cyber warfare.

The High-Level Committee on Programs (HLCP) discussed the risks and impact of cyber-crime and cybersecurity on the United Nations system during its' 20th session. During its' 22nd session, the HLCP agreed to set up the UN Group on Cybercrime and Cybersecurity to acknowledge program policy aspects of cybercrime and cybersecurity. Their mission was to develop coordination and collaboration on these issues within the UN.

During the 24th session, HLCP assigned the group to create a draft policy on cybercrime and cybersecurity that focused on how the UN could popularize issues of cybersecurity and cybercrime and encourage programs to focus on it.

The HLCP took note of the draft policy and progress made by the UN Group on Cybercrime and Cybersecurity, which focused solely on the cybersecurity and anti-cybercrime capabilities of Member States rather than the internal needs of the UN. The International Telecommunication Union and the United Nations Office on Drugs and Crime were charger with further developing and improving the policy.

According to a 2011 Norton study, threats to cyberspace have increased drastically in the past years affecting 431 million adults globally, equating to 14 adult victims every second and one million cybercrime victims every day.

The United Nations Economic and Social Council (ECOSOC) held a special event on "Cybersecurity and Development" to address this issue. They aimed to bring awareness at the international policy level by providing members of ECOSOC a summary of the situation currently at hand. They wanted to point out some of the obstacles ahead in the areas of cybersecurity and crime. In addition, they also wanted to identify a range of practice policies and initiatives around the world that could aid in building a culture of cybersecurity. Finally, they wanted to explore options for a global response to the growing rates of cybercrime.

CHARGER MUN
UNIVERSITY OF NEW HAVEN • NOTRE DAME HIGH SCHOOL

Additional Research

In addition to the research previously mentioned please make sure that you continue to direct your research to what the United Nations has already done regarding this topic. One area to look at is the UN High-Leven Committee on Programmes. This committee is not limited to issues of cybersecurity, however, they have consistently discussed such topics.

The United Nations backs a cybersecurity alliance known as IMPACT, International Multilateral Partnership Against Cyber Threats, founded in 2008. IMPACT is the first public-private union that is against cyber threats and is known for being a neutral ground to bring governments together. IMPACT began approaching the issue of cybersecurity by signing a cooperation agreement between Rome and INTERPOL in 2012. On this level, forensics and analysis of any malware would be communicated confidentially between INTERPOL and IMPACT at least once a year, while also preparing for future circumstances.

Another place to look in regards to the UN is the UN International Telecommunications Union's Global Cybersecurity Index (GCI). We would encourage all of you to understand the research and information being taken in this index and how it is being used in order to address cybersecurity issues.

As a Delegate, it is important to understand policies within your own country and those that your country may see eye-to-eye with. We encourage you to prepare and to be knowledgeable about the state you are representing and their own national policies. As a simulation of the real United Nations, we strongly encourage all delegates to focus on being inclusive of other delegates, and cooperative with others in efforts to solve these real-life world issues. These are the most important values of the UN and therefore should be a guiding principle for all delegates.

Additional Sources:

https://www.itu.int/pub/D-STR-SECU

https://www.itu.int/pub/D-STR-CYB_CRIME-2015

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

https://dig.watch/processes/ungge

https://www.unodc.org/southeastasiaandpacific/en/what-we-do/toc/cyber-crime.html