CHARGER MUN
UNIVERSITY OF NEW HAVEN • NOTRE DAME HIGH SCHOOL

United Nations Security Council 1

Welcome Delegates to the second annual Charger Model United Nations. We are excited to work with you as your dais and look forward to the work you will produce.

The chair for this committee is Laura Fruzzetti. Laura recently completed her bachelor's degree in Criminal Justice from the University of New Haven and has participated in their Model United Nations program for three semesters, including one as Head Delegate. The co-chair for this committee is Shivani Patel. Shivani is pursuing her degree in Criminal Justice and has participated in the University of New Haven's Model United Nations program for two semesters. We are thrilled to be your Dais for the Security Council.

The topic before the Security Council is:

Cyber Security in the Digital Age

ChargerMUN will take place on December 9th, 2018 and will run between three sessions: Formal Debate, Moderated Caucus, 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 encourage all delegates to read and familiarize themselves with the official ChargerMUN rules prior to attending the conference. Understanding that each delegate embodies the beliefs of unique national governments while often encompassing the views of progressive people, we encourage you to remain cooperative and inclusive throughout the conference. Throughout the day, you will hear and deliver speeches, engage in negotiations, write clauses, and propose creative solutions with your fellow delegates. We ask you all to recognize that the tendency in the actual UN is to pass only one resolution among the entirety of the body of Member States within the committee. If you are to have any questions regarding our expectations of your diplomacy, please do not hesitate to approach the Dais. We are very much looking forward to meeting each of you and seeing your diligent work over the course of the conference.

CHARGER MUN
UNIVERSITY OF NEW HAVEN • NOTRE DAME HIGH SCHOOL

Committee Overview

Following the end of World War II, the five main victors, known as the permanent five (P5): China, USSR (Russia), France, the United Kingdom, and the United States, sought to find a peaceful means for solving the real-world issues that led to the war. Through this, the United Nations was created. The Security Council is a vital part of the functionality of the United Nations and its rules of procedure and structure differ greatly from the other organs within the United Nations.

As the charter states, the purpose of the Security Council is to, "investigate any dispute or any situation which might lead to international friction or give rise to a dispute, in order to determine whether the continuance of the dispute or situation is likely to endanger the maintenance of international peace and security." In fulfilling its purpose, the Security Council must respond to such situations by investigating any situation threatening international peace; recommending procedures for peaceful resolution; calling upon other Member States to completely or partially interrupt economic relations as well as sea, air, postal and radio communications or to sever diplomatic relations; and enforcing its decisions militarily, if necessary. Due to the seriousness of the issues brought before the Security Council, its solutions, unlike those of other committees, are binding. This means that if a resolution passes, all Member States in the United Nations must abide by what the document says.

The Security Council consists of the P5 Member States, which never change, and ten temporary Member States. These temporary Member States are chosen and distributed based on geographical location. There are five Member States from Africa and Asia, one from eastern Europe, two from Latin America and the Caribbean and two from Western Europe, ensuring that each area is partially represented. 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 the 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 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

The first computer virus ever used was created in 1971 and since then breaches on cybersecurity have become more sophisticated and dangerous. With continuing technological advances, cyber terrorists have more means and opportunity to potentially cause major harm to a country and its citizens by just using cyber means. This can include situations where classified information is leaked to the public, personal information about the government and a country's situation is hacked and used for malicious means, and cyber hacking is used to control important technology that may affect the safety of a country and its citizens.

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 information communication technologies (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.

We are currently living in the digital age, a time where technological advances continue at exponential rates. If security measures are not put in place and actions are not taken to keep up with the "times" the world will be at risk. Though technology, can make life easier and civilization more advanced, cyber terrorists can also use the same systems to destroy any sense of security that we as people currently have. It is up to the security council to look into ways to keep up with the cyber abilities in order to ensure that citizens' most basic and fundamental rights are preserved and protected.

CHARGER MUN
UNIVERSITY OF NEW HAVEN • NOTRE DAME HIGH SCHOOL

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.

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. Ban Ki-Moon assembled a group of experts to comprise a report entitled "On the Developments in the Field of Information and Telecommunications in the context of International Security" that studied "possible cooperative measures in addressing the existing and potential threats". The report found that there was a need to elaborate confidence-building measures and "norms, rules or principles of responsible behavior of states".

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.

At the summit of the Group Eight industrialized countries, former President Barack Obama and Russian President Vladimir Putin announced that they had approved the first ever bilateral agreement on confidence-building measures on the cyber spectrum. These measures address information exchange and crisis communication. Cyber-specific crisis communications were established, specifically a channel between computer emergency response teams (CERTs) that represented two countries that would discuss malware stemming from both of their respective states.

There are many factors that make the situation in cyberspace difficult to control. With the constant absence of a secular understanding of the applicable international rules for state behavior in that domain, many of the tools can be used for both legitimate and illegitimate purposes. Things like global connectivity, vulnerable technologies, and anonymity aid the spread of disruptive cyber activities that may cause a considerable amount of damage, like spreading malware into networks or digital control systems.

CHARGER MUN
UNIVERSITY OF NEW HAVEN • NOTRE DAME HIGH SCHOOL

Current Situation

Cybercriminals, hackers, cyber terrorists and nation states all contribute to the current issue of cybersecurity. Cybersecurity attacks cause billions of dollars in loss each year and today it is easy to hack into things like cars or phones. One of the most significant problems is a lack of knowledge about cybersecurity.

To address this issue, 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 popularize issues on 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

As part of your research, we highly recommend all delegates completely understand and utilize the policies and practices that their Member State already has in place. However, research should not be limited to just your own Member State. It is your job to understand the actions taken by Member States you have partnerships, agreements and/or similar viewpoints with. By directing your focus to these areas of research you will be able to identify more creative and probable solutions to the issue of cybersecurity in the digital age.

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. One of the most recent discussions included the Action on Cyberspace, biotechnology, and New Weaponry. Such research will provide you with an idea of how the UN acts on topics regarding cyber matters.

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.

Though we have given you a few ideas on where to direct your research it is imperative that you look further than what we have highlighted in this background guide. The more you know the easier the conference will be. We wish you all the luck in your research and we look forward to meeting you in December. Finally, and most importantly don't forget to have fun!

Further Sources:

http://www.un.org/en/sections/un-charter/chapter-v/index.html

https://www.un.org/press/en/2014/gadis3512.doc.htm

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx