CSPCMUN2017

Disarmament and International Security Committee

Committee: The United Nations Disarmament and International Security Committee

Topic: Addressing the Importance of Cyber Security in the Future

Director: Gerardo Contreras

Moderator: Andrea Torres

"Men make history and not the other way around. In periods where there is no leadership, society stands still. Progress occurs when courageous, skillful leaders seize the opportunity to change things for the better." – Harry S. Truman

Dear Delegates,

First of all, welcome to CSPCMUN2017. It is an honor to have you in this year's edition. We hope that this simulation is a memorable experience. We are confident that during these three days you will develop skills such as leadership, negotiating, and critical thinking while representing a specific country. We expect that in this model you meet new people who will encourage you to make an impact in our world. I am sure that you will prepare yourself enough so you can get to agreements and help in the resolution of the committee's problematic. We hope that you enjoy this simulation as much as we will. Any doubts you may have, do not hesitate on asking us.

Sincerely,
Mariana Lazo
Chief of Moderators

I. Committee Overview

DISEC is the first committee of the General Assembly. This committee discusses issues of diplomatic and military stability with goals of disarmament and increased international security, which can lead to a wide variety of potential threats to global peace. It considers all disarmament and international security matters relating to the purpose of any other committee of the United Nations. This committee also works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament. Also, DISEC deals with issues regarding the promotion, establishment, and subsequent maintenance of global peace while simultaneously working to prevent weapons proliferation.

It is important to remember that this committee will be responsible for making recommendations for action: DISEC, as part of the General Assembly, is never authorised to declare sanctions, make war, or impose other regulations on nations.

In this simulation, delegates will consider two topics that relate very immediately to the peace and security of the world. It is crucial to emphasise the importance of focusing on the security aspect of these topics.

II. Topic information

A) History of Topic

Cyber criminals are becoming more agile and their attacks are coming more frequently than large companies are able to keep up; and traditional methods, like anti-malware softwares, are no longer efficient enough to keep delicate data safe. To help with this problem, many forward-thinking executives are using automation as a tool for safer defense against these attacks.

Cyber attacks usually aim towards credit card information, customer data, money, and carrying out industrial espionage.

Until a few years ago, most companies and organizations were adequately prepared for an attack of this sort; now a stunning 90% state that "they are insufficiently prepared for a cyber attack" in The Global Risks 2015 report. The

sudden lack of security against these attacks was caused by the use of machines commonly known as bots.

Its personnel are no match for these bots, as they are machines who can do hundreds of lines of coding in a matter of seconds.

Unfortunately, Cyber crime costs an average of US$400 billion per year, according to estimates by the Center for Strategic and International Studies, causing many companies to not be able to pay for the necessary equipment against these attacks.

There is still a lot of work to be done, and the organizations being attacked have to catch up to the people behind these cyber attacks

B) Current Issues

United States of America: In past years, United States has became the country that has more cybercrime. This is because it is the Global leader country ; they have all the technological resources available. Recently, Russia had been hacking the US. Russia tried to hack the elections so Donald Trump could win. Because of the results, the CIA has been going deep with this issue , but the chief of CIA just told that if US tries to hack Russia for revenge, could lead to a cyberwar.

Canada: In Canada, it was just discovered that they had under dozens of state-sponsored hackers, which had affected in power plants, electrical grids, aviation software. A variety of government-run systems were facing assault from Advanced Persistent Threat (APT) technology, likely dispatched by foreign governments both hostile and friendly. This had affected the measures of security Canada has to take.

Russia: Now, Russia is getting to hack all the countries to get to know the weak points of the countries, an example is in the U.S. elections between Hillary Clinton and Donald Trump. Russia got interest of having Donald as a president for their good, because Donald wanted to be allied with Russia and vice versa. So, it has been said that Russia could interfere in the voting results.

Germany: The German Government has been developing a major programme to protect its computer networks and supply systems for any kind of cyber attack. A

new institution - the National Cyber Defence Centre (Nationales Cyber-Abwehrzentrum) – will be responsible for detecting potential threats, analyzing them and coordinating the necessary measures to disable the threat. In addition, a National Cyber Security Council will be established.

C) UN Action

Due to the fact of the importance of this problem, the UN has been working hard for the past years and they have been negotiating about the solution of this topic. The UN group of governmental experts on cybersecurity agreed on a substantial and forward-looking consensus report. It represents an important achievement for the maintenance of international peace and stability in this new and crucial area. For the United Nations, it was difficult and people spend a lot of time addressing this new international security challenge.

III. Conclusion

To conclude, this problem needs to start getting solved. This dilemma can affect companies, people, business, and even the government. They can be affected by identity theft, fraud, extortion, malware, pharming, phishing, spamming, spoofing, spyware, troyano, viruses etc.. By exposing even a small amount of private information of an individual, incites the world to start a war or revelion.
Nowadays, we live in the era of technology, and internet is our more vulnerable piece of our lives. In the internet there are passwords for our credit cards, payments , etc.

IV. Essential Questions

1. What is the percentage of vulnerable companies in your country?
2. How much does your country spend protecting from cyber attacks?
3. How many attacks did your country had in the past years?
4. How does your nation has been impacted?
5. Why is your delegation being affected by this problem?
6. How does your delegation government should assist the people that have been affected?
7. Have others helped your country with this issue? In which ways?

8. Has your delegation established any organizations, reforms or projects to protect citizens against cyber risks?

V. Resources

"Cyber Risk." *Cyber Risk*. N.p., n.d. Web. 08 Nov. 2016.

Scott Charney - Corporate Vice President, Trustworthy Computing. "The University's Role in Addressing the Future of Cybersecurity." *Microsoft Secure Blog*. N.p., 2014. Web. 08 Nov. 2016.

Burrington, Ingrid. "The Internet Apocalypse Map Hides the Major Vulnerability That Created It." *The Verge*. N.p., 2016. Web. 08 Nov. 2016.

"A Guide to Cyber Risk - Allianz Global Corporate & Specialty." N.p., n.d. Web. 8 Nov. 2016.