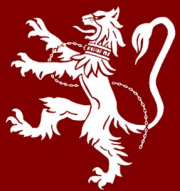




PEA  MUN

Chair:
Sherry Lim

Co-Chair:
Alexis Gorfine

Vice Chair:
Justin Psaris

Security Council

Cyber Security

PEAMUN VIII
October 30, 2016

A Letter from the Chair

Security Council

Dear Delegates,

Welcome to the eighth annual Phillips Exeter Academy's Model United Nations Conference. My name is Sherry Lim and I will be chairing this year's Security Council along with Alexis Gorfine and Justin Psaris on Cyber Security. We are excited to have all of you engage in an intense and a fruitful debate. We sincerely hope that with your enthusiasm and participation, we can make this one day conference an unforgettable and a priceless experience.

We will be focusing on topics regarding Cyber Security such as but not limited to: finding balance between protecting the citizens' rights to privacy as well as ensuring security from unwanted online attacks, the problems of responsibility, comprehensive approach towards national security, state sovereignty, as well as the protection of critical infrastructure, systems, networks, goods and values, and the safety of individuals.

In the 21st century information and communication technologies (ICTs) are permeating and transforming every aspect of our lives. The increasing extent of ICTs has far exceeded national and international regulations governing them. Individuals, organisations and countries must take actions to improve the way that technological and cyber-risks are managed.

We hope that your experience at PEAMUN will further help you to improve as a delegate in MUN, but also to become a better global citizen and raise awareness about global issues that impact our daily lives. If you have any questions we are more than happy to answer your questions so email any one of us: clim1@exeter.edu , agorfine@exeter.edu , jpsaris@exeter.edu.

Thank you for your time and dedication. We wish all of you the best of luck on your preparation for this committee and I look forward to seeing you!

Sincerely,

Sherry Lim, Chair

Description of the Committee: Security Council

The Security Council has the primary responsibility for the maintenance of international peace and security. It has 15 Members, and each Member has one vote. Under the Charter, all Member States are obligated to comply with Council decisions. The Security Council takes the lead in determining the existence of a threat to the peace or act of aggression. It calls upon the parties to a dispute to settle it by peaceful means and recommends methods of adjustment or terms of settlement. It dispatches military operations, imposes sanctions, mandates arms inspections, deploys election monitors and more. In some cases, the Security Council can resort to imposing sanctions or even authorize the use of force to maintain or restore international peace and security. The Security Council also recommends to the General Assembly the appointment of the Secretary-General and the admission of new Members to the United Nations. And, together with the General Assembly, it elects the judges of the International Court of Justice.¹

General Information:

What is Cyber Security?

According to International Telecommunication Union (ITU), cybersecurity is defined as

“the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.”

¹ <http://www.un.org/en/sc/>

Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, integrity, and confidentiality.”²

Since 2014, the rate of cybersecurity incidents has risen by over 38%, and malicious cyber attacks cost \$300 billion to \$1 trillion USD per year. Global cyber activity has a cost rivaling that of the global drug trade. The most profitable type of cybercrime, identity theft, generates almost \$1 billion a year.³

Though the vast majority of companies and individuals state concern over cybersecurity, only a few have taken action and preventative measure. Everyone is at risk of cybercrime, and top intelligence officials of the U.S.A. believe that cyber attacks and digital spying pose a greater threat to national security than terrorism.⁴

Terms/Definitions:

Cyber Risks

Risks of financial loss, or damage in the reputation of an organization due to a failure of information technology systems.

Cyber Crime

² <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>

³ "The Economic Impact of Cybercrime and Cyber Espionage." McAfee.
<http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>.

⁴ "Cyber Security Primer." What Is Cyber Security? Accessed June 29, 2016.
<http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm>.

Mostly conducted by individuals or organized groups in order to extract money, data or cause disruptions.

- ex) a) obtaining credit/debit card data and intellectual property
- b) hindering the operations of a website or service.

Cyber War

A nation ordering destruction and espionage against another nation to cause disruption or extract data.

Cyber Terrorism

There is no agreed definition on Cyber Terrorism. However, it is argued that cyberterrorism has complementary purposes to those of real-world terrorism. The main motivations for these attacks are social, economic and political issues. Cyberterrorism aspires to shut down important national framework, such as government affairs, energy and transportation to alarm and threaten the community.

Modern tools of Cyber Terrorism

Botnets

Botnets, or “Bot Networks,” are made up of vast numbers of compromised computers that have been infected with malicious code, and can be remotely-controlled through commands sent via the Internet. Hundreds or thousands of these infected computers can operate in concert to disrupt or block Internet traffic for targeted victims, harvest information, or to distribute spam, viruses, or other malicious code.⁵ Botnets have been described as the “Swiss Army knives of the

⁵ Weimann, Gabriel. *Terrorism in Cyberspace: The next Generation*. New York, NY: Columbia University Press, 2015.

underground economy” because they are so versatile. Botnet designers, or “botmasters”, can reportedly make large sums of money by marketing their technical services. For example, Jeanson Ancheta, a 21-year-old hacker and member of a group called the “Botmaster Underground”, reportedly made more than \$100,000 from different Internet Advertising companies who paid him to download specially-designed malicious adware code onto more than 400,000 vulnerable PCs he had secretly infected and taken over. He also made tens of thousands more dollars renting his 400,000-unit “botnet herd” to other companies that used them to send out spam, viruses, and other malicious code on the Internet. In 2006, Ancheta was sentenced to five years in prison.⁶

Hactivism

Hactivism which is a combination of hacking and social activism, is defined as the use of digital tools in pursuit of political ends and/or social change.⁷ The earliest examples of hactivism date back to 1999, when the loose network known as the Cult of the Dead Cow created "Hactivismo", and organisation which espoused that freedom of information was a basic human right. The group designed software to circumvent censorship controls on the Internet which some governments used to prevent citizens from seeing certain content. In recent years, hactivism has been applied more widely to protests against governments, multinational organisations, governments as well as rural law enforcement agencies. The tactics of hactivists now include denial of service attacks on sites, as well as leaks of confidential documents to the

⁶ 5 Bob Keefe, “PC Security Still More of a Wish than a Promise,” Atlanta Journal, February 3, 2007, 1A; U.S.

⁷ http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hactivist/?_r=1

public. While hacktivists tend to go after non-retail organisations, the fallout from these attacks can still affect millions of people.⁸

Anonymous, the internationally renowned hacktivist group established in 2003, is one of the many groups dedicated to fighting Internet censorship around the world. The group uses DDoS attacks in order to cripple websites of companies which advocate internet censorship.⁹ During a DDoS attack, servers are constantly asked for information and services from hundreds of sources to the point where they cannot process the inquiries and then freeze. Once their targets are disabled, the Anonymous group displays its iconic message and makes public private information. This can range from addresses and passwords to classified security documents online. Much like other hackers, Anonymous publishes the botnets and methods used for the attack after it has been successful. Anonymous has claimed responsibility for hacking at least 15 countries' government websites in the first eight months of 2012.¹⁰

Past Efforts on Cybersecurity: Introduction

With the ever-expanding importance and usage of the internet,¹¹ comes the increased emphasis on cybersecurity. According to a study conducted by IBM and Ponemon Institute in 2015, the expenses that result from data breaches have reached a startling 3.79 million dollars worldwide.¹² It is further estimated that this will become a 2.1 trillion dollar problem by 2019.¹³ With the increasing threat of cyber crime, not only are smaller businesses and individuals investing more

⁸ http://www.pcworld.com/article/239594/how_hacktivism_affects_us_all.html

⁹ "How Hacktivism Affects Us All." PCWorld. Accessed August 22, 2016.

http://www.pcworld.com/article/239594/how_hacktivism_affects_us_all.html.

¹⁰ <http://www.computerworld.com/article/2899040/anti-censorship-group-in-china-faces-ddos-attack.html>

¹¹ <http://www.statista.com/statistics/273018/number-of-internet-users-worldwide/>

¹² <https://securityintelligence.com/media/2015-ponemon-cost-of-a-data-breach-study/>

¹³ <https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/>

in their own protections due to technological security developments made available to them,¹⁴ but major organizations such as the United Nations (UN) and individual countries themselves are also increasing their investments in cybersecurity.

Past Efforts on Cybersecurity: United Nations

The United Nations first addressed the issue of cybersecurity in January of 1999 through Resolution 53/70 which resulted in international security advancements of information and telecommunication.¹⁵ More developments occurred throughout the next four years that continued to demonstrate the ongoing international UN efforts in cybersecurity.¹⁶

In 2007, the UN specialized community, The International Telecommunications Union (ITU), created the ITU Global Communications Agenda (GCA) which focuses on developing “legal measures, technical & procedural measures, organizational structures, capacity building, and international cooperation,” in the field of cybersecurity.¹⁷ Furthermore, the GCA has since created initiatives such as the Child Online Protection, erected in November of 2008, aimed at providing a safe online environment for children.¹⁸ ITU has also established the Global

¹⁴ http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf

¹⁵ http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70

¹⁶ http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

¹⁷ <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>

¹⁸ http://www.itu.int/en/cop/Pages/about_cop.aspx

Cybersecurity Index (GCI), a way of measuring a country's level of cybersecurity development through analysing their work in each of the aforementioned GCA focus categories.¹⁹

In 2013, the UN demonstrated that it was still staying up to date in the evolving field of cybersecurity. The committee members acknowledged the importance of privacy and “affirm[ed] that the same rights that people have offline must also be protected online, including the right to privacy.”²⁰ This resolution calls upon all states to “respect and protect privacy” and “to take measures to put an end to violations of those rights and to create the conditions to prevent such violations.”²¹

Past Efforts on Cybersecurity: Nations Collaborating Globally

Not only has the UN been working vigorously to keep up with cybersecurity measures, but nations throughout the world have been developing policies to manage the changing realm.

The United States alone increased their cybersecurity spending 76% to \$3.34 billion in 2015.²² In 2015, The White House and Congress collaborated to create and pass The Cybersecurity Act of 2015 which overall increases the level of the nation's cybersecurity.²³ However, President Obama doesn't believe that this act is enough; therefore, the Obama administration is attempting to implement the Cybersecurity National Action Plan (CNAP); this is a long term plan that will

¹⁹ <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>

²⁰ http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

²¹ Ibid.

²² <http://www.tridentcybersecurity.com/wp-content/uploads/2016/02/Increased-Spending-in-Cybersecurity-Drives-Surge-in-Funding.pdf>

²³ <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

“enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security.”²⁴ Looking ahead, the American federal government is focusing on protecting their infrastructure; advancing the identification and reporting of cybersecurity breaches; collaborating internationally “to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.”²⁵ To accomplish these goals, the U.S. has worked to educate citizens about cyber threats and has created a more comprehensive partnership with the private sector.²⁶

Individual nations, such as the United States of America, have developed their own policies on cybersecurity. What is perhaps more significant, however, is the collaborative work that has been done between countries.

In 2015, G20²⁷ leaders agreed upon the notion that no nation should steal intellectual property of any sort through means of cyberspace. This agreement is an important step in cybersecurity, helping advance the process of global acceptance that international law is applicable to cyberspace conduct.²⁸

In addition to the agreement in the G20 conference, nations have been collaborating to create cyberspace behavior norms. In the United Nations Group of Governmental Experts, the United

²⁴Ibid.

²⁵ <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity>

²⁶ Ibid.

²⁷ G20 is a group of nations who collaborate on solving issues related to world economic development and international economic relations

²⁸ <http://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace>

States proposed regulation agreements that were adopted into the UNGCE's consensus report, stating:

“first, no country should intentionally damage the critical infrastructure of another state or impair the use of critical infrastructure that provides services to the public; second, no country should take actions intended to impair the Computer Security Incident Response Team (CSIRT) of another country from responding to cyber incidents and that such CSIRTs should be not be used to do harm online; and third, countries should cooperate with requests from other states to investigate cybercrimes and mitigate malicious cyber activity emanating from their territory.”²⁹

Furthermore, in 2015, the United States and China developed a cyber agreement, which President Obama announced in September. The agreement was focused on the promise that neither nation would “conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage.”³⁰ Additionally, the two governments would respond and aid one another in cybercrime investigations, set norms for cyberspace behaviors, and create a hotline between the U.S. and China to deal with issues accordingly and collaborate on creating a better cyber relationship.³¹

Soon after, China and the U.K. also entered into a cybersecurity agreement. England's Prime Minister David Cameron and China's President Xi Jinping followed the U.S. and China agreement by agreeing not to spy on one another through cyberspace. Both sides aim for this

²⁹Ibid.

³⁰ <http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/>

³¹ Ibid.

agreement to abolish cyber attacks and unapproved access to intellectual property and private information. This agreement signals a growing relationship between the two nations, as it is accompanied by China's plan to invest in the future of the U.K., helping to finance a nuclear power plant that will be built in 2025.³²

Challenges to Cybersecurity: Cyber Attacks and Breaking Pacts

Despite frequent collaboration between nations on cybersecurity efforts, there have, unfortunately, been many incidents of cyber attacks by one nation onto another.

Estonia

In 2007, Estonia became victim to a cyberattack. The attack shut down ministry, bank, media, and political party websites by using Distributed Denial of Service (DDoS), causing websites to overload and shut down.³³ Fortunately, the attack didn't cause too much destruction in the country, only causing economic damage and hassle for officials and citizens. Different European countries came to Estonia's assistance, as did the Computer Emergency Response Team (CERT) from the Ministry of Economic Affairs and Communications.³⁴ Furthermore, NATO CERTs and the European Network and Information Security Agency (ENISA) from the UN came to provide additional aid to Estonia. This breach in cybersecurity was addressed not only by the victim nation but additionally by foreign nations.³⁵ This demonstrates the international collaborative

³²<http://www.scmagazineuk.com/china-and-the-uk-sign-cyber-security-agreement/article/448578/>

³³http://www.clingendael.nl/sites/default/files/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf

³⁴ Ibid.

³⁵ Ibid.

effort against cyber threats. Since the attack, The Estonian Ministry of Foreign Affairs has noted the significance of cybersecurity and have addressed the issue multiple times diplomatically and politically in the EU and in NATO. Furthermore, Estonia has increased investments in the NATO Cooperative Cyber Defence Centre of Excellence in Estonia in the following years.³⁶

Saudi Arabia

Another significant cyber attack in recent years occurred in Saudi Arabia in 2012, demonstrating the power of cyberattacks, and addressing one of the prominent challenges of cybersecurity: cyber attacks often target one group or organization but have unintended consequences by affecting many other cyber users.³⁷ In 2012, the largest company in Saudi Arabia and state oil company, Saudi Aramco, was targeted, affecting 85% of the company's technology.³⁸ Not only did this attack damage technology in Saudi Arabia, but it also affected foreign offices in other regions of the world. While the attack was focused on interrupting the production of Saudi Aramco's products, it only disrupted office computers, avoiding effect on production. To deal with the attacks, Saudi Aramco shut down their computer systems so as to prevent the virus from spreading. With the systems down, they replaced or restored the infected computers. While the Ministry of the Interior stated that the attacks was exteriorly driven, this event was publicized as an interior issue. The Ministry of the Interior aided Saudi Aramco post attack by helping them discover who the attackers were; this information, however, was never publicized.³⁹

³⁶ Ibid.

³⁷https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

³⁸https://www.clingendael.nl/sites/default/files/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf

³⁹ Ibid.

The United States

In September of 2012, the United States also faced a cyber attack, one that was considered to be the “biggest cyberattack in history.”⁴⁰ The perpetrator committed a DDoS attack against America’s top six banks, Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank, and PNC Bank, causing the banks’ websites to be incredibly slow and temporarily inaccessible to customers. Fortunately, the attacks were only a nuisance, and no data was stolen.⁴¹ Soon after the attack, a group called Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the attack⁴² which they labelled “Operation Ababil.” In the next weeks, more attacks followed aimed at banks and large corporations.⁴³ However, many experts claim that the Izz ad-Din al-Qassam Cyber Fighters couldn’t have committed the attack, as it was too complex for an organization such as their own to have performed. Politicians and government officials immediately pinned the attacks on Iran, a nation who was avenging themselves after they were placed under Western economic sanctions due to their highly opposed nuclear program.⁴⁴ To aid in the aftermath of the attacks, several government agencies and ministries provided their various services. To respond to the attacks, The State Department requested help from multiple different countries, asking them to shut down any identified malicious computer codes from their servers.⁴⁵

⁴⁰ <http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/>

⁴¹ <http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/>

⁴² Ibid.

⁴³ <https://security.radware.com/ddos-knowledge-center/ddospedia/operation-ababil/>

⁴⁴ https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

⁴⁵ <http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/>

The United States suffered another cyber attack in 2014 when Sony Pictures Entertainment was hacked by “Guardians of Peace.” In November, the hackers released various confidential data from Sony’s servers. Additionally, malware was installed into the computers, designed to eliminate all computer server data.⁴⁶ To halt the attack, the hackers demanded monetary gains, continuing to release data until they received their demands. By December, the hackers stopped demanding monetary funds, instead demanding the cancellation of the movie, “The Interview,” a comedy about U.S. T.V. personalities traveling to North Korea to assassinate Kim Jong-un. Soon after, the hackers began threatening moviegoers as well, writing, "Remember the 11th of September 2001. We recommend you to keep yourself distant from the places [movie theatres screening “the Interview”] at that time."⁴⁷ Following these threats, many theatres decided not to screen the film. After the top theatres, Regal Cinemas, AMC Entertainment and Cinemark Theatres, announced their postponement of the screening, Sony was forced to cancel the film’s release.⁴⁸ Eventually, the FBI concluded that North Korea was behind the attacks; however, North Korea denied all accusations. By December 23rd, Sony executives recalled their decision to cancel the film, and decided to continue with the Christmas screening in a few theatres and online.⁴⁹ This example of a cyber attack is an important one, demonstrating the power of cyberattacks to make Americans question and almost recall their own rights to freedom of speech and press, or in the case, freedom of film.

⁴⁶ <http://www.bbc.com/news/world-us-canada-30526406>

⁴⁷ <http://www.bbc.com/news/world-us-canada-30526406>

⁴⁸ Ibid.

⁴⁹ <http://www.bbc.com/news/world-asia-30608179>

China and America Relations

In 2015, right after the Chinese-American cybersecurity agreement, China attempted, multiple times, to hack into American companies' servers to heist intellectual property. Over the course of a few weeks, over seven attacks against technological companies and pharmaceutical companies were documented; the targets of these attacks made it evident that this wasn't China gathering national security intelligence, but rather China stealing exactly what they had just promised not to steal in the cybersecurity agreement.⁵⁰ Unfortunately, this is an example of a situation in which a nation broke their commitment to the predetermined cybersecurity agreement. Fortunately, this is a rare case and there are consequences to China's actions. This example is crucial, however, as it is important to comprehend that despite being successful most of the time, cyber agreements aren't the complete solution to this growing problem. It is necessary to continue advancing technologies to increase protective methods and to continue collaborations across nations to build trust and to create a more secure cyber world.

Possible Solutions:

The United Nations Security Council is responsible for addressing issues concerning international peace and security, and cybersecurity is one of the most dangerous and threatening. To prepare for committee deliberations, Member States should consider the need for:

- A global cybersecurity agreement.
- The creation of virtual task forces to target internet facilitated organized crime.

⁵⁰<http://www.pbs.org/newshour/making-sense/despite-cyberagreement-chinese-cyberattacks-u-s-companies-continue/>

- Education on protection from cyber threats.
- Encouraging/requiring individuals and companies to invest and improve cybersecurity.
- Computer system leaders to improve cybersecurity.

Questions to think about:

- What defines cybersecurity, cybercrime and cyberterrorism?
 - How do international and domestic laws affect cyber criminals/cyberterrorists, and how should they affect them?
 - Will threats of violence be enough to be regarded as cyberterrorism?
- What steps has your country taken to address cyber security? Have these actions been synonymous with recommendations from organizations (NGOs, other countries)?
- Should cyberterrorists and terrorists be treated the same way?
- Are cyber attacks an act of war as defined by the laws of armed conflict?
 - How should the attribution of cybercrimes be dealt with?
- Should a UN forum be created to guide and deliberate on issues of cybersecurity?
 - How should this forum operate?
- Should a international governing body be created to form a legal framework on cybersecurity?