Committee: ITU

Topic: Addressing Breaches of Intergovernmental Cyber-Ware

Report of the Chairs

I. Theme of the Conference

Model United Nations San Antonio (MUNSA) is a conference dedicated to fostering authentic and passionate debate amongst delegates in order to generate solutions to current global issues. The theme of *MUNSA XXIV: Envision* encaptures our mission to urge delegates to foresee a future in which these problems have been dissolved. With collaboration in mind, delegates from every committee are encouraged to visualize innovative resolutions and a prosperous world to come. Together, we will propel ourselves into an age in which brilliant ideas converge to transform our world and address its most paramount issues.

`

II. Rationale

Higher level action is required when cyber-ware is breached on an intergovernmental level. Cyber-tactics in intergovernmental cyber-ware is a breach of systems that needs further surveillance. In a truly modernized world, it is vital to secure government records, as this information could easily fall into the wrong hands in the event of a security breach. All nations with extensive cyber security infrastructures are at risk of a violation. This committee will work to visualize a brighter future in which countries are efficiently able to address cyber-ware breaches.

III. Background of the Topic

Intergovernmental is defined as relating to or conducted between two or more governments.[4] Cyberware is defined as anything that has access to the internet. The need for a strong cybersecurity infrastructure first began in 1988 when the Morris worm, a type of malware, infiltrated the world's cyberinfrastructure. This worm was predominantly spread around the U.S and slowed down computers to the point of being unusable.[6] In 2009, a group called the Iranian Cyber Army hacked a popular Chinese search engine, Baidu.[2] These events struck fear in the

hearts of many world leaders and increased global urgency to establish a stronger cybersecurity infrastructure.

These issues have been addressed in a multitude of ways. Many countries have legislation in place to combat cybercrimes, such as Penal codes and anti-cybercrime acts. Countries with strong cybersecurity programs have many awareness programs and initiatives for higher education in cybersecurity for government contractors. Many countries also have partnerships internationally through an initiative known as ITU impact, a program that provides necessary aid to countries in terms of cybersecurity in the event of an intergovernmental breach. This program also facilitates aid between countries for matters of cybersecurity.

IV. Contemporary Evidence of the Topic

With the number of cyber-attacks increasing in frequency, establishing adequate prevention is critical. As many networks become interconnected and more organizations build onto their existing infrastructures, the opportunities for adversaries to connect to, infiltrate, and access information increases[1]. Since networks have no borders, every country is at risk of being targeted[1]. In the past, various nation-states have targeted governments, militaries, and commercial networks. In terms of risk, particularly in the case of national security, the cost is hard to calculate. As a result, governments have become increasingly involved in trying to limit the risk. Every nation dreams of being the most progressive. Since people live in a truly digitized world, nations achieve this through cyber breaches.

Many countries are a part of the ITU impact program. These countries have partnerships internationally and spend long periods of time refining their cybersecurity infrastructure to ensure maximum privacy and prevent breaches. Reaching a solution is imperative, as a world with intergovernmental cyber breaches is a world without privacy. Solving cyber ware breaches not only makes the world more private and secure, but it also has the capability to end low education rates and unemployment with its creation of jobs in the IT sector[3], a field that is in very high demand. Addressing the breaches of intergovernmental cyber ware will solve a multitude of global problems and create a more prosperous and secure planet for many generations to come.

V. References and Research Resources

1. (2017, October 31). Cyber Security: How Government Can Combat Cyber Threats. Retrieved from https://careersincybersecurity.com/cyber-security-and-its-role-in-government/
2. Danchev, D. (2010, January 12). Baidu DNS records hijacked by Iranian Cyber Army. Retrieved from https://www.zdnet.com/article/baidu-dns-records-hijacked-by-iranian-cyber-army/
3. (2017, May 12). How cybercrime and cybersecurity affects nations and geopolitics ». Retrieved from https://www.crowdstrike.com/blog/cybercrime-cybersecurity-affects-nations-geopolitics/
4. (n.d.). Intergovernmental. Retrieved from https://www.merriam-webster.com/dictionary/intergovernmental
5. (2017, March 18). Retrieved from https://www.cybersecurity-review.com/tag/intergovernmental/
6. Nato. (n.d.). The history of cyber attacks - a timeline. Retrieved from https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

VI. Note to the Delegates

Greetings Delegates,

The chairs of ITU would first like to thank you for participating in MUNSA XXIV. We hope that this conference allows you to gain valuable experience in a world that is filled with technology. Furthermore, we are looking forward to meeting you this January and are excited to hear what you bring to the debate! If there are any questions or comments, please do not hesitate to contact us at:

Emma Williams: ewilliams7983@stu.neisd.net

Rishith Telakalapalli: rtelakalapa9451@stu.neisd.net

Andres Rivera: arivera7929@stu.neisd.net

VII. Director General Contact Information

Joseph Ruelas - jruelas4856@stu.neisd.net

Dana Marion - dmarion0455@stu.neisd.net