Committee: General Assembly (DISEC)
Agenda B: Battling Breaches in Cybersecurity

I. Introduction

We wouldn't reveal our personal information if we know that ours will be used for commercial purpose. Unfortunately, such hypothetical situation became a reality, and became known as the "Facebook Scandal". In this scandal, according to the New York Times, Cambridge Analytica was alleged for attempting to create a psychological database by accessing millions of Facebook users' personal information. This company was initially allowed to use this source only for a research purpose. However, when their act of information-abuse was exposed to the public, Facebook inevitably had to endure both domestic and international backlashes simultaneously. Afterwards, more people became suspicious of Facebook's cybersecurity policy so that it had to conduct its cybersecurity reform. This cyber threat didn't only occur on a national level. Also, recently in the United States, cybersecurity company called Symantec claimed that Chinese hackers associated with the Chinese government intelligence hacked into the database of NSA. Even Pentagon, the headquarters of the United States Department of Defense, stated and warned the cyber espionage of the Chinese government for extracting technologies for military purpose. Eventually, these cases led to an increased awareness of the public, which made Facebook and the US government reconsider their systems built for protecting data and privacy. People called out for stricter regulations on firms' activities regarding the use of personal information in the cyber web and a stronger cyber defense system for US government associated facilities. Clearly, as technological advancement, an increase in social media users, and globalization are in progress, supplementing the existing cybersecurity has become crucial. As more information is being shared in cyberspace, it does provide benefits to people looking for diverse resources, but, it can also make personal information and data vulnerably placed in the cyberspace to be abused. Thus, delegates in this committee must come up with effective solutions to counter the breaches in cybersecurity in both the national and international level.

II. Definitions of Key Terms:

Cybersecurity:
Cybersecurity is a protection against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. With the increasing scope and significance of cyberspace, more emphasis is being placed on cybersecurity, which helps prevent cyberattacks, data breaches, and identity theft. For example,

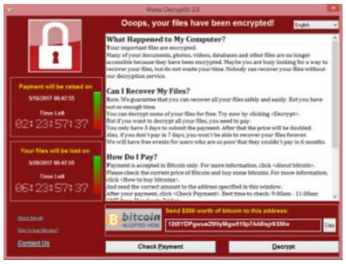
in case of the United States, President Donald Trump previously signed the Cybersecurity and Infrastructure Security and Agency (CISA) Act of 2018 to establish the agency devoted to defending the U.S. infrastructure and to train workers of the government and private companies to be prepared to handle cyberattacks.

Cyberattacks:

Cyberattacks, also known as Computer Network Attacks(CIA) are collective attempts by hackers to destroy or damage technology-dependent enterprises and networks. They usually use malicious codes to alter computer codes, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. For instance, Ddos attack is one of the main examples of Cyberattacks. Ddos (Distributed Denial of Service) attack is a cyber-attack in computing, where the perpetrator disturbs the networks of an online service to temporarily disrupt services and target important resources from banks, news websites, and government facilities.

Ransomware:

Ransomware is a type of malware that threatens to temporarily or perpetually block access to victim's data unless a ransom is paid. In some cases, a more advanced malware uses a technique called cryptoviral extortion, which malware encrypts the victims' files and data and demand a ransom payment for the decryption key or code. A ransom payment is made by using cryptocurrency to make tracing nearly impossible. Recently in 2017, a type of ransomware dubbed "Wanna Cry" put the world into chaos by making a lot of financial loss for the victims. According to the National Law Review, the largest agencies struck by ransomware were National Health Service hospitals in UK that was affected by up to 70,000 devices, including computers, MRI scanners, blood-storage refrigerators, and theatre equipment.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

[illegible]

Data Breach:

A data breach is a security incident in which information is accessed without authorization. Data breaches occur in a variety of ways for diverse purposes. For example, Hackers attack seemingly vulnerable systems to seek personally profitable information comprising identities to use it for commercial purposes. Data breach is considered hazardous since it can damage lives and reputations and take time to repair.

Data breach even happens between countries to hack other nations' military information for their advantage.

III. Background Information:

Cybersecurity has been a well-known issue after the World Wide Web was created by Tim Bernes Lee in 1991. This establishment made information available anytime, anywhere for Internet users. Users felt comfortable for the convenience of transferring and sharing information without any limitation. However, as more and more information overflew in the internet, hackers found means to unlawfully obtain private information. Although technologies to reinforce the pre-existing cybersecurity were developed, malware and hacking technologies were improved exponentially at the same time. Recently, the ransomware strike "Wanna Cry" led hackers to gain access to great amounts of personal data and files, hospital records, and train systems etc. Not only that, information collected from firms was often abused. As the Facebook case would address, customer's credibility toward Social Networking services have decreased in terms of data protection.

IV. Previous actions and efforts of the United Nations

International effort to reduce problems related to the threat of cybersecurity started from 1980. That was when the Organization of Economic Cooperation and Development (OECD) proposed several guidelines called "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data". These guidelines claimed that the consent of individuals—users of social media and firms—should be involved. Also, these guidelines assured that collected data and information will be used only for the original purpose of firms and social medias. Afterwards, the General Assembly agenda in 1998 became a trigger to tackle the problems occurring in cyberspace although the outcome of its attempt was minimal: collecting more specific information than national reports only with the state information security.

In 2004, the General Assembly First Committee installed the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security(GGE). It produced guidelines and recommendations regarding norms and principles of state behavior and accountability for their actions in the digital sphere. Although this attempt paved an innovative way for the cybersecurity, Russia, US, and western allies had different notions on the regulation of personal information so it couldn't conclude a productive outcome until 2009. To be more specific, GGE had a meeting even after 2009 and raised a crucial point in the 2010 report (A/65/201) concerning the "increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes." The United Nations have been working even up until today to propose effective solutions to reduce problems related to cybersecurity.

V. Major Countries and Organizations Involved

China

China is known for its notorious reputation regarding disputes of intellectual property rights. According to several Internet media, the Chinese government was involved in the process of extracting and hacking other countries' data and intellectual property rights. Especially, the United States accused the Chinese government and Huawei, a Chinese IT company, guilty for hacking information of a multinational telecommunication company, Nortel executives and planned documents for future products in 2004. Recently, the Chinese government seems to be undergoing the reform of cybersecurity policy. It claimed that its new cybersecurity law would demand companies, both Chinese and multinational, to cooperate with the government and provide "unspecified data for technical support." The law also imposes mandatory testing and certification of computer equipment for critical sector network operators. China states that the inherent purpose of this project is data protection; however, corporations can't easily overlook its hidden plan for data breach and infringement of private information.

European Union

European Union has put much effort to reduce problems related to cybersecurity. First, it established the European Union Agency for Network and Information Security(ENISA) in 2004 with the ends to detect and prevent breaches of cybersecurity. ENISA specifically focused on developing cybersecurity strategies. In 2012, ENISA initiated the European Cyber Security Month, a forum to discuss issues regarding cybersecurity. European Cyber Security Month produces a deployment report, which outlines plans and strategies for initiating transitions in cybersecurity, that helps other European countries to undergo transitions to prepare their cybersecurity system for future cyberattacks. Also, the European Union initiated the EU General Data Protection Directive (GDPR), which focuses on guaranteeing the individuality and freedom of information storage and data. Under this directive, involved organizations are required to utilize data for authorized purposes and to ensure the data's accuracy. It is mandatory for the involved organizations to adopt at least one encryption method for their database.

United States

As president Barack Obama stated, for the United States, a digital infrastructure is their “strategic national asset”. Also, as a predecessor in cybersecurity technology, US has been accusing China for the repeated cyberespionage and criticizing China for hacking their firms’ technologies and designs. However, interestingly, US was accused for its cyberattacks attempt even before the exposure of the Prism scandal, a program that collected Internet communications from various US Internet companies. United States had disputes, not only with China, but also with other countries such as Iran. United States received suspicion for conducting a cyberattack against the Iranian nuclear facility, as over one thousand Iranian nuclear centrifuges have been destroyed. However, the specific countries involved in the cyberattack against Iranian nuclear facilities were never confirmed.

Russia

Russia, along with other strong IT countries, relies heavily on information technology. Russia initially performed DDos attacks on Estonian government in 2007. Many experts claimed Russia’s movement as a revenge against political tensions. Also, in 2017, several US intelligent services claimed that Russia intervened in the 2016 Presidential election by hacking mails of the Democratic National Committee. Although not completely affirmed, many are suspicious of Russia for engaging in several other political conspiracies.

VI. Future Outlook/ Solutions

The entire globe could not harvest a significantly successful outcome from previous UN conferences to improve cybersecurity. One of the struggles for the progress of international cooperation was that countries were hesitant to share their network system and information database. Thus, to facilitate the international cooperation among member states, it is first important to build a system or institution where countries can transparently share their information—but not to the extent of confidential information.

Second, the committee should devise effective solutions to reduce the gap in the level of technological advancement among countries worldwide. According to the Global Cybersecurity Index (published in 2017), developing countries tend to “lack well-trained cybersecurity experts as well as a thorough appreciation and the necessary education on cybersecurity issues for law enforcement”. Although there are several countries, such as Singapore and the United States, which have a strong cybersecurity foundation, because the security system is interconnected among countries, all member states should have stronger technologies.

Third, the prevention of proliferation of malicious ICT (Information and Communication Technology) should be achieved. As more terrorist organizations and hacking groups place their interest in cyberspace, all member states should be especially careful not to let their advanced technologies fall into the wrong hands. Thus, there should be an international institution that can detect the spread of malicious technologies and restrict the development of technologies.

Last but not least, on a domestic level, institutions solely for surveillance on data collecting and usage of the firms should be established immediately. Facebook Scandal broke out since there was no sufficient surveillance on the usage of stored information by Facebook. Thus, by establishing an institution for surveillance, firms will be able to regularly keep track of their usage of database.

VII. References

Biomteric Signature ID Staff. “GDRP Compliance and You.” Biometric Signature ID. 14 May 2018. Web Accessed 26 May 2018. https://www.biosig-id.com/resources/blog/292-gdprand-you

Collier, Kevin. “Chinese Spies Stole NSA Hacking Tools, Report Finds.” *CNN*, Cable News Network, 15 June 2019, edition.cnn.com/2019/05/07/politics/china-nsa-hacking/index.html.

“Cryptoviral Extortion.” *Wiktionary*, en.wiktionary.org/wiki/cryptoviral_extortion.

European Union Staff. “European Union Agency for Network and Information Security (ENISA).” Europe.eu. 22 May 2018. Web Accessed 22 May 2018. https://europa.eu/europeanunion/about-eu/agencies/enisa_en

European Union Staff. “Timeline of Past Events.” Europe.eu. 2016. Web Accessed 28 May 2018. https://www.enisa.europa.eu/topics/cybersecurityeducation/european-cyber-security-month/timeline-of-pastevents

Houser, Kristin. “The US Finally Has a Defense Agency Devoted to Cybersecurity.” *Futurism*, Futurism, 20 Nov. 2018, futurism.com/cybersecurity-us-defense-cisa.

Huifeng, He. “Chinese Cybersecurity Law Causing 'Mass Concerns' among Foreign Firms .” *South China Morning Post*, 1 Mar. 2018, www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china.

“IWonder - Timeline: How Stuxnet Attacked a Nuclear Plant.” *BBC*, BBC, www.bbc.com/timelines/zc6fbk7.

Millar, Sheila A. “WannaCry: Are Your Security Tools Up to Date?” *The National Law Review*, 22 May 2017, www.natlawreview.com/article/wannacry-are-your-security-tools-to-date.

NortonOnline. “What Is a Data Breach?” *Official Site*, Symantec Employee, us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html.

“Obama: From Now On Digital Infrastructure Treated As Strategic National Asset.” *CircleID Master*, Circle ID Reporter(Annonymous), www.circleid.com/posts/20090529_obama_digital_infrastructure_strategic_national_asset/ https://intpolicydigest.org/2019/05/13/what-china-s-cybersecurity-law-says-about-the-future/.

Rosenberg, Matthew, et al. “How Trump Consultants Exploited the Facebook Data of Millions.” *The New York Times*, The New York Times, 17 Mar. 2018, www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardian*, Guardian News and Media, 17 May 2007, www.theguardian.com/world/2007/may/17/topstories3.russia.

“What Is a Cyberattack? - Definition from Techopedia.” *Techopedia.com*, www.techopedia.com/definition/24748/cyberattack.