COMMUN VII

2022 | Commonwealth School, Boston

Crisis Committee: Cybersecurity

Background Guide

Committee Head: Mirai Duintjer Tebbens Nishioka

Welcome Letter

Dear Delegates,

My name is Mirai Duintjer Tebbens Nishioka, and I am a sophomore at Commonwealth. I was involved in COMMUN last year and have been participating in Model UN since middle school. As the world went online in 2020 due to the COVID-19 pandemic, the use of online services has skyrocketed, increasing the importance of cybersecurity. You may have heard of various hacks and cybersecurity issues over the past year, from the Colonial Pipeline attack to the Twitch hack to the Log4j vulnerability. As more and more people come to rely on the internet and the damage caused by cyberattacks increases, the need for unified action against cybercrime has increased drastically.

In this committee, you will be representing a diverse group of countries and companies faced with the issue of cybercrime. The committee will be set in the present day but you will be faced with unique fictional crises. We can't wait to see what solutions you come up with!

This committee will require a position paper to be submitted in order to be eligible for awards. We look forward to seeing your unique take on the crisis and learning more from you on your country or company's relationship to it. If you have any questions, please email me or my fellow crisis members at mnishioka@commschool.org, hlevenson@commschool.org, aghosh@commschool.org, or tdu@commschool.org.

Cybersecurity - Crisis Committee

> "I think computer viruses should count as life. Maybe it says something about human nature, that the only form of life we have created so far is purely destructive"
>
> -Stephen Hawking

Background:

This committee was convened after a major hack of Facebook's website, which showed the words "We Hacked Facebook" to all visitors of the website. In addition, a small number of users' personal data was released to the public, though a Meta representative stated that the hackers "likely had access to up to 100,000 users' data". The hack was resolved after Meta paid a sum of 1,000 bitcoin (roughly equivalent to 40 million US dollars) to the perpetrators of the hack. It is currently unknown what person or organization perpetrated the hack, but it seems that it was perpetrated by a previously unknown hacker or hacker group as the word "shapeless" was found in Facebook's website code after the hack.

As a delegate in this committee, you will be representing a country, tech company, or security company and your goal will be to stop the perpetrators of the Facebook hack and prevent similar hacks from happening in the future. We hope your diverse companies and countries will come together to devise plans that combat hacking and neutralize this new threat.

Discussion:

The word "hacking" has roots in English as a pejorative term. Originally, the word meant "to work on something without a constructive benefit." This definition was used as a self-deprecating mode of address by MIT students, where it took on the meaning of performing technical work for no benefit but for pleasure. This was the first noted instance of a modern usage of the word "hacker", and as time progressed, the use of the word became more mainstream. From there, the word has been split between two meanings in relation to cybersecurity: that of "black hat" hackers who are associated with malevolent and dangerous behavior, and the less common definition of "white hat" hackers. The latter is distinguished to have less dangerous intentions than their "black hat" counterparts, but this term has fallen out of use and been replaced with new terms carrying less negative connotations.

The growth of hacking has been tightly linked to the increased use of computers. One of the first forms of hacking was developed in the 1950's, as phone calls were being routed using tones of specific frequencies, a group of people known as "phone phreaks" emerged, who emulated these frequencies to place free calls. One famous "phone phreak" was John Draper, who used toy whistles from Cap'n Crunch cereal boxes to hack the phone system. During the early days of "phone phreaking", the biggest computers were part of the phone system. At this time, "phone phreaking" was mostly a method of exploring computers and not an illegal way of making money. However, as "phone phreaking" advanced and devices called blue boxes were made to generate the tones needed to hack the phone system, the government started cracking down on phreaks and fining or arresting them.

While a proposed concept following the invention of the first computers in the 1940s, hacking would not become a threat until a few decades later. This is due to the fact that the computers of this era were primarily used for accounting and lacked the means to easily interfere with other computers. The 1960s and 70s saw an increase in availability and decrease in size of computers-albeit they were still difficult to attain even among programmers. However, with the introduction of the ARPANET (internet precursor), disruptive programs came into place alongside antiviruses. It was the birth of cybersecurity.

As computer technology continues to progress, so does the threat of hacking. In contrast to the 1900's, where personal computers were scarce, the 21st century saw the emergence of increasing reliance on the internet. With more people connected to the internet, hackers have more opportunities to try to infiltrate people's privacy. Anyone, even those who spend little time online, is susceptible to the threats that hackers pose. Common threats to security include fake spam emails, instant messages, or websites that deliver dangerous malware to one's computer.

While computer software (and security) has become more advanced, the overreliance on the internet for data storage has the potential for considerable problems. Every day, 2.5 quintillion bytes of data are collected, including passwords, emails addresses, and any type of personal information. Depending on the website or company, this data is stored in different ways, but it is all digital and, thus, potentially prone to hacking. A single security breach can leak thousands of passwords, causing severe damage to personal security. In more serious cases, entire IT systems may be hacked causing shutdowns to major services such as utilities, government offices, and hospitals.

Today hackers and their cybersecurity counterparts use increasingly complex algorithms, encryptions, and computers to try and overtake the other in a constant game of cat and mouse, or, perhaps more accurately, snakes and newts. Modern hackers may hold systems or data ransom, encrypting it so as to render it unusable and releasing it only after the ransom is paid. These ransoms are almost always in the form of cryptocurrencies, a virtual currency that runs on a block chain. These block chains allow transactions to be conducted anonymously and securely, with complete anonymity and no centralized body, a perfect tool for criminals to transfer money.

Blockchains are not the only new technology with the potential to change the state of cybersecurity; quantum computers have the potential to revolutionize encryption. A quantum computer, at a basic level, is a computer capable of performing certain types of calculations much faster than conventional binary computers. A malicious actor, with a powerful enough quantum computer, like those in development by several countries and companies, could theoretically break any currently used encryption, no matter how complicated. Likewise, a quantum computer could also be used to create an encryption unable to be broken by anything but another quantum computer. However, quantum computers are only in their infancy and developments such as these described are a significant amount of time and money away, if possible at all.

Roles & Portfolio Powers:

Countries & Unions

As a representative of a country or a union of countries, you have the power to make decisions on the behalf of them. This includes but is not necessarily limited to:

- Creation or utilization of cyber divisions of your military/government
- Passing laws, regulations, and signing treaties with other nations
- Utilizing your country's judicial systems and militaries
- Collaboration with other nations or companies

When preparing for your role, you should be sure to look not only at your country's cybersecurity resources but also at their history of cyber warfare and cyber criminals within their borders.

Country / Union	Information
Brazil	In Brazil, cybersecurity requirements are provided by regulatory agencies, such as the central bank (BACEN), the Securities and Exchange Commission (CVM), the National

	Telecommunications Agency (ANATEL) and the Brazilian Private Insurance Authority (SUSEP). In order to improve strategic infrastructure for communications, energy, transport, finance, water and other essential parts of Brazil's national security, sovereignty, integration and economic development, Brazil is making an effort to strengthen regulations on cybersecurity, requiring regulated entities to implement robust cybersecurity policies.
China	With a drive to become a technologically advanced economy, China, along with the United States, is on the forefront of the global technological boom. However, unlike the United States, China's government places an emphasis on control, and frequently censors information from within or outside of its borders. This control is not absolute, though, as a Cybersecurity Law enacted in 2016 created the principle of cyberspace sovereignty, defined security obligations of internet providers, refined rules surrounding personal information protection, and instituted rules for the transmission of data from critical information infrastructure.
European Union	The European Union Agency for Cybersecurity (ENISA) contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for cybersecurity threats. As cyberattacks and cybercrime are increasing in number and sophistication across Europe, a stronger cybersecurity response to build an open and secure cyberspace will create greater trust among citizens in digital tools and services and help prevent disaster.
India	India is the world's second most populous country, and the largest democracy by far. Though it lags behind many other nations in terms of technological development, it still plays an important role on the world stage. Cyber crime and other forms of hacking and scams are prevalent in India, and measures must be taken to prevent the growth of such an industry. During the COVID-19 pandemic, India's cyber security industry nearly doubled in size, with revenues from cybersecurity products and services growing from $5.04 billion to $9.85 billion in 2 years.
Israel	Lying in the center of the cybersecurity industry, Israel is one of the few countries that face hundreds and thousands of cyber-attacks every month on its government websites and data systems. In order to prevent disasters from cyber-attacks, Israel's government has made efforts to improve Israel's rapidly growing cyber security industry. In addition, Israel has invested into education for its people to make them technologically empowered with skills and expertise so that they can fulfill their

	ambitions.
Japan	Cybersecurity in Japan has been given increased attention in response to a rise in the frequency and sophistication of cyber attacks. These attacks have created major concern for the safety of infrastructure sectors that are reliant on technology, a large portion of Japan's economy. Japan's National Center for Incident Readiness and Strategy for Cybersecurity (NISC) is the leading agency in the Central Government in forming the national cybersecurity strategy. Additionally, the NISC guides all Central Government agencies in establishing and implementing cyber security policies and measures. In 2019, the NISC announced its National Strategy for Cyber Security, which identifies an urgent need for reinforcing cybersecurity measures in all levels of Japanese society and in all aspects of technological development.
Russia	Russian military theorists conceptualize cyber operations within the broader framework of information warfare, a concept that includes computer network operations, electronic warfare, psychological operations, and information operations. In the past, it has been claimed that Russia has organized a number of denial of service attacks as a part of their cyber-warfare against other countries. Most notably, they have been accused of influencing the recent elections in the United States with cyber attacks.
Ukraine	In order to guarantee Ukrainian national security, the development of a national cyber security system is vital, especially in this current time of crisis. Ukraine's national security confirms a high threat level related to transnational cyber crime and attempts by foreign governments, organizations and individuals to use modern information technologies against the state. Thus, to prevent the modification and leakage of data and the obstruction of critical infrastructure processes, Ukraine has begun developing cyber defense mechanisms and procedures.
United Kingdom	The United Kingdom aims to lead responsible and democratic cyber power, so that they can protect and promote their interests in and through cyberspace and in support of national goals, such as the strengthening of structures, partnerships, and networks necessary to support a societal approach to cybersecurity.
United States	One of the largest, most technologically advanced countries in the world, the United States is home to some of the world's most important technological companies. Because of this, the United States leads the world in strengthening security, resilience, and workforce of the cyber ecosystem to protect critical services and

	the American people, with cyber divisions in both the military and government. The United States is also a major competitor with China.

Companies

Companies can often move faster and have more unrestricted access to data than nations. Thus, they are an integral part of this committee. As a representative of a company, you have the power to make decisions on the behalf of them. This includes but is not necessarily limited to:

- Any decisions about company policies and products
- Utilization of cyber divisions of your company
- Collection and analysis of data
- Collaboration with other companies or nations

When researching your role, you should be sure to take note of your company's assets, data, and cybersecurity. You should also note your company's ability to track and prevent hacking.

Company	**Information**
Amazon	The largest e-commerce company in the world, there is no doubt that Amazon has completely revolutionized shopping and commerce on the global scale. In this way, Amazon walks the line between a physical company, with massive and controversial warehouses, and an online one, with huge amounts of data and various products available for purchase.
Cloudflare	Cloudflare is one of the largest website security companies in the world. Cloudflare provides services to companies to protect their online presences from attacks such as DDoS (distributed denial-of-service). With their expertise in this area, they may be able to research and track the perpetrators of the recent attacks against Meta.
Huawei	The Chinese technology company Huawei is the second largest technology company based outside of the United States (Sony is the first, for those of you wondering.) It is also one of only two companies in this committee based outside of the United States. Huawei is the largest smartphone manufacturer in the world and a major provider of hardware around the world. Many have questioned Huawei's connection to the Chinese government and it remains highly controversial, especially in the West.
IBM	IBM has been a giant in the technology industry for decades. It provides a wide variety of services to clients such as hardware, software, and consulting. IBM is also a major research institution. In the past, it has invented the ATM, floppy disk, and barcode, to name a few. Today, it is one of the leaders in AI and quantum computing research.

Kaspersky Lab	Russian based Kaspersky Lab develops and sells antivirus software and other cybersecurity products. Kaspersky Lab's Global Research and Analysis Team is at the forefront of the discovery of viruses and other malware and has tracked down the perpetrators of a number of cyberattacks. Kaspersky Lab has been criticized by some for its alleged involvement with the Russian government.
Meta (formerly Facebook)	Meta is one of the largest companies in the world and the vast majority of its assets are cyber-adjacent. With billions of users and huge amounts of information collected on each of them, data and cyber security are central to Meta as a company. Along with this massive platform, Meta has also had its share of controversies. In addition to the earlier Cambridge Analytica and whistleblower scandals, Meta now faces the data breach that has caused the current committee to convene.
Microsoft	Second only to Apple in market cap, Microsoft dominates many areas of the hardware and software markets. The price of this domination is being targeted by viruses and other attacks. Historically, Microsoft technologies have been far more prone to attacks than their competitors.
Raytheon	Raytheon Technologies Corporation is an American aerospace & defense company based in Massachusetts. It is one of the largest aerospace, intelligence services providers, and defense manufacturers in the world, and works closely with the US and other allied governments to provide the cutting edge in cyberspace technology, both offensive & defensive.

Bibliography

Research:

- History of hacking: https://courses.cs.washington.edu/courses/csep590a/06au/projects/hacking.pdf
- USA Government Cybersecurity: https://www.ibm.com/security/services/us-federal-cybersecurity-center
- History of cybersecurity: https://blog.avast.com/history-of-cybersecurity-avast
- Genealogy of hacking: https://journals.sagepub.com/doi/pdf/10.1177/1354856516640710

Sources

"Impact of digital surge during Covid-19 pandemic - NCBI." 9 Jun. 2020, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7280123/ Accessed 1 Jan. 2022

"Pipeline Attack Yields Urgent Lessons About US Cybersecurity." 8 Jun. 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. Accessed 2 Jan. 2022.

"Twitch source code and creator payouts part of massive leak." 6 Oct. 2021, https://www.theverge.com/2021/10/6/22712250/twitch-hack-leak-data-streamer-revenue-steam-competitor. Accessed 2 Jan. 2022.

"A Log4J Vulnerability Has Set the Internet 'On Fire' | WIRED." 10 Dec. 2021, https://www.wired.com/story/log4j-flaw-hacking-internet/. Accessed 2 Jan. 2022.

"Hacker Lexicon: What Are White Hat, Gray Hat, and Black ... - WIRED." 13 Apr. 2016, https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/. Accessed 27 Feb. 2022.

"Kaspersky Lab Has Been Working With Russian Intelligence." 11 Jul. 2017, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence. Accessed 28 Feb. 2022.