International Telecommunication Union (ITU)

Background Guide Topic:

Combating Cyberattack

Senzoku Gakuen Model United Nations March 26-27, 2022
jmmunadmin@senzoku.ac.jp

Director's Note

Welcome to the ITU Japan Metropolitan Model United Nations Conference! My name is Imari Nagase and I am beyond thrilled to be this year's Intermediate II Director. I cannot wait to see you all virtually!

I was born in Japan and spent six years in an international school. Becoming friends with people from diverse nationalities was an experience that could not be replaced, and was one of the incentives for me to join the MUN club. I am so grateful to be able to chair this conference even with the delegates who live thousands of miles away from Japan. Sadly, due to the ongoing pandemic, many of us have lost the chances of directly meeting other delegates from around the world. I was also helpless to attend Global Classrooms International MUN in 2020. However, I have been engaged with various MUN club activities since my first year in Senzoku Gakuen. Along my MUN journey, I was able to encounter amazing people and open my eyes to the challenges society faces today. This is my first time chairing or directing a formal conference, but along with the two co-directors of this committee, we can bring you all a fun and memorable experience!

With more than 4 billion people having access to the internet, cyberthreats have become a pressing issue for not only governments, but also to each and every individual. Moreover, social media plays a role in allowing hackers to target and exploit the vulnerable. I am afraid even I have received a few sketchy emails that claim I can win a thousand dollars if I click on a red button. Because it is an issue that pertains to all sorts of stakeholders, I highly encourage delegates to research this topic from all sorts of angles.

I look forward to the heated discussions and negotiations that I am sure will occur in the conference!

Sincerely,

Imari Nagase, Director
International Telecommunication Committee
Senzoku Gakuen Model United Nations Club
Japan Metropolitan Model United Nations 2022

Introduction of the Committee

Marcel Thué established the International Telecommunication Union in 1865 with the goal of connecting the world in numerous ways.[1] One of which is to facilitate easier communication and connection between people. There are 193 member states and over 900 companies, organizations, and academia involved in the ITU. More specifically, there are companies based on Telecoms, the internet, broadcast, satellite, software, Artificial Intelligence, FinTech, utilities, automotive, and smart cities. [2] ITU works closely with industries, public and private sectors, to "define the new technologies that will support tomorrow's networks and services."[3]

Key Terms

Buffer Overflow attack: the most common DoS attack that occurs when a program is able to write more data to a buffer than it was originally designed. This allows the excessed data to overflow into adjacent buffers, overwriting its contents and enabling the attacker to have access to the flow of the program.[4]

Cyber threat actors: any person or persons who attack an organization's cybersecurity with malicious intent.[5]

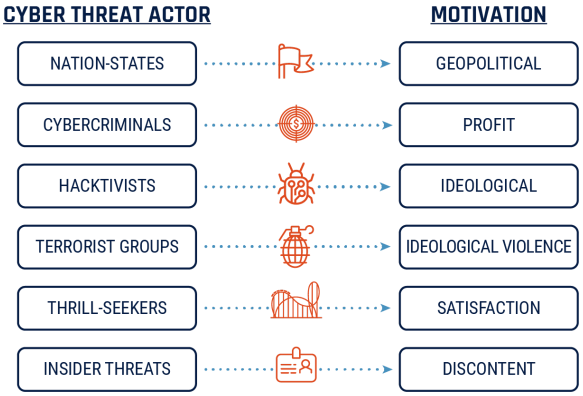

Figure 1: Specific Cyber Actors and the motivations [6]

Data Theft: the act of stealing data intentionally.[7] Identity thefts related to tax and finance such as bank accounts is also an

[1] *Discover ITU's HISTORY* . ITU. https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx.
[2] *About*. ITU. www.itu.int/en/about/Pages/default.aspx.
[3] *Our Vision*. ITU. www.itu.int/en/about/Pages/vision.aspx.
[4] Malkiewicz, K. (March 8, 2021) *This Year (So Far) in Buffer Overflows*. Dover Micro Systems. https://info.dovermicrosystems.com/blog/2021-buffer-overflows.
[5] *What Is a Threat Actor and Why Should You Care?* Sophos Home. home.sophos.com/en-us/security-news/2021/what-is-a-threat-actor.aspx.
[6] *Cyber Threat and Cyber Threat Actors*. Government of Canada, cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.
[7] *Cybersecurity Glossary of Terms*. Global Knowledge. www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/#gref.

issue. Children are taken advantage of their naivety by identity thieves. [8]

Denial of service (DoS) attack: an attack meant to restrict the intended user's access to the internet and computer by "flooding the target by traffic, or sending it information that triggers a crash." [9]

Distributed Denial of service (DDoS) attack: a type of an attack that takes advantage of the specific capacity limits that apply to any network sources, such as infrastructure that enables a company's website. [10]

Malware: a short for malicious software. Typically used as a comprehensive term that refers to any software designed to cause damage to a single computer, server, or computer network.

Ransomware: an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. By using ransomware, the attackers are able to make money as cheaply as possible. [11]

Internet Protocol (IP): a unique set of numbers that identifies a device on the internet or the local network. [12]

Current Situation

History of the Problem

Cyber threats only came to light decades after the computer was first invented by Charles Babbage. In 1972, The Advanced Research Projects Agency Network (ARPANET), a research project, proved that viruses can indeed exist.

Moreover, in 1988, the first case of a hostile exploitation of buffer overflow occurred. [13] A cyber worm called "the Morris worm" attacked 6,000 of the approximately 60,000 computers that were then connected to the internet. The extent of damage swelled up to millions; some institutions wiped their systems and emails were delayed for weeks. Robert Tappan Morris, the culprit of the incident, was found guilty, making him the first person sentenced under the 1986 law

[8] *15 Facts You Have to Know About Identity Theft.* Lifelock. www.lifelock.com/learn-identity-theft-resources-facts-you-have-to-know-about-identity-theft.html.

[9] *What is a Denial of Service Attack-Palo Alto Networks.* Paloalto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

[10] *What is a DDoS Attack? - Meaning of DDoS.* Kaspersky. https://www.kaspersky.com/resource-center/threats/ddos-attacks

[11] *Ransomware 101.* CISA. https://www.cisa.gov/stopransomware/ransomware-101

[12] What is an IP Address - Definition and Explanation. Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

[13] *Buffer overflow.* Wikipedia. https://en.wikipedia.org/wiki/Buffer_overflow#History

which outlaws unauthorized access to protected computers.
Ever since then, governments have established laws and international treaties to ensure the safety of its citizens.

Problems

Cyber attacks is a term encompassing various types and purposes. Malware, DDoS, Phishing, SQL injection attacks, Cross-site scripting (XSS), and Botnets are typical and damaging examples of Cyber attacks.

Figure 2: Types of Cyber Attacks

Security teams often encounter disadvantageous situations against the attackers for they have to defend many of their attack points; while the attacker only needs to find one weakness.[14]
Cybercrime is harder to tackle than other criminal activities for being borderless. This "poses severe problems for law enforcement since previously local or even national crimes now require international cooperation."[15]
In addition to being harder to police and prosecute, COVID-19 measures have also been affected by cyber attacks and contributing to its rise in crimes. The COVID epidemic forced officials to embrace new solutions quickly, and resulted in a 600 percent increase in data hacking alone. Furthermore, in late 2020, UK vaccine maker AstraZeneca was targeted by North Korean cyber attackers for their vaccine information.[16] Also, the situation that remote workforces are increasing creates more soft spots for cybercrimes.[17]

Motives

There are multiple reasons that actors might engage in cybersecurity violations. Below is a short list, followed by case studies of specific crimes.

Attacks Toward Businesses

Financial purposes are most common. Criminals may want things such as business'

[14] Michael. C. *6 common types of cyber attacks and how to prevent them.* TechTarget. https://searchsecurity.techtarget.com/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them.

[15] Dennis. M.A. (September 19, 2019) *Cybercrime.* Encyclopedia Britannica. https://www.britannica.com/topic/cybercrime.

[16] Raymond. P. *Cybersecurity Threats to the COVID-19 Vaccine.* F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/cybersecurity-threats-to-the-covid-19-vaccine.

[17] Rob. S. (March 16, 2019) *134 Cybersecurity Statistics and Trends for 2021.* Varonis. https://www.varonis.com/blog/cybersecurity-statistics/.

and customers' financial details, sensitive personal data, clients lists, and intellectual property.[18]

Attacks Toward Personal Devices

According to IPA(Information-technology Promotion Agency), primary purposes of attacking personal devices include: smartphone payment abuse for money, phishing for personal information, and slandering to mentally damage the target. [19]

Motives on Geopolitical Espionage

Cyber espionage is a type of cyberattack in which an unauthorized user attempts to access sensitive information or classified data for economic gain or political advantage. Assets such as political strategies, affiliations, and military intelligence are stolen by executing an APT (Advanced Persistent Threat) attack, which are carefully planned to infiltrate a specific organization and evade security measures for a decent amount of time.

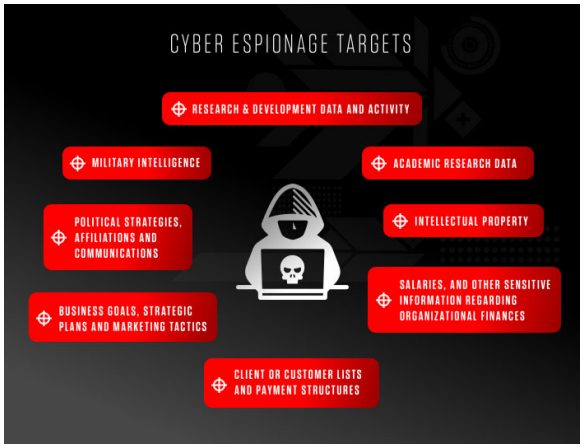

Figure 3: Cyber Espionage Targets [20]

Case Studies

Subtopic I: Tackling Cyberterrorism and warfare

The Fight Against Ransomware

CISA (Cybersecurity and Infrastructure Security Agency) introduces ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable."[21] By using ransomware, the attackers are able to make money as cheaply as possible.

Case Study 1: Anonymous (Hacker Group)

[18] *Cybersecurity for Business*. Invest Northern Ireland. https://www.nibusinessinfo.co.uk/content/reasons-behind-cyber-attacks.

[19] (July 30, 2021) *情報セキュリティ10大脅威2021*. Information-technology Promotion Agency Japan(IPA) https://www.ipa.go.jp/security/vuln/10threats2021.html.

[20] *What is Cyber Espionage?* Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

[21] *Ransomware 101*. CISA. https://www.cisa.gov/stopransomware/ransomware-101

Figure 4: Anonymous Symbol[22]

An amorphous group of hackers who call themselves "Anonymous" gained media attention when, in 2008, a series of Distributed Denial of Service (DDoS) attacks were used against the Church of Scientology. A few of the organization's websites went offline. According to a website controlled by Anonymous, its goal was to "save people from Scientology by reversing the brainwashing." [23]
The leaderless organization has attacked a number of websites ranging from governments to small organizations. For example, the group has targeted the Ku Klux Klan and taken down terrorist groups' twitter accounts. [24] Moreover, in 2011, Egyptian government websites were shut down by Anonymous until President Hosni Mubarak resigned. [25] Anonymous has even hacked into the dark web and published over 1500 users' data who visit child pornography websites. The list of Anonymous' operations goes on. However, regardless of the intention behind the hacking, it is still a dangerous form of expression that poses a threat to people's daily lives. Some Anonymous hackers have been arrested. According to an FBI agent, "we've dismantled the leaders of Anonymous."[26]

In 1984, the U.S. congress passed the Computer Fraud and Abuse Act (CFAA). This act makes activities conducted by organizations like Anonymous illegal. More specifically, it criminalizes the act of intentionally having access to a computer

[22] *Anonymous (Hacker Group).* Wikipedia. en.wikipedia.org/wiki/Anonymous_(hacker_group).
[23] PCWorld. (January 28, 2008) *Hackers Hit Scientology With Online Attack* ABC News. abcnews.go.com/Technology/GadgetGuide/story?id=4194143.
[24] Rory. C. (November 17, 2015) *Anonymous Takes on IS*. BBC News. www.bbc.com/news/technology-34850573.
[25] *Hacktivism 101: A Brief History and Timeline of Notable Incidents - Wiadomości Bezpieczeństwa*. Hacktivism 101. www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/hacktivism-101-a-brief-history-of-notable-incidents.
[26] Smith. G. (December 7, 2017) *FBI Agent: We've Dismantled The Leaders Of Anonymous.* HuffPost. www.huffpost.com/entry/anonymous-arrests-fbi_n_3780980.

"without authorization." [27] Because of the vague notion of "without authorization" which the CFAA did not define, many prosecutors abuse this. For example, prosecutors bring charges against individuals which do not align with the culpability Congress wanted to address when it passed the law.

The vague language used in cybersecurity laws is not unique to U.S. legislations. In fact, according to the Human Rights Watch, policies that deal with cybercrime often use "vague and ill-defined terms to criminalize legitimate forms of online expression." [28] There are even countries that do not have any laws covering cybercrime and the protection of personal information. Namibia is one example of this. The country has become one of the "most targeted countries in Africa by cyber criminals." [29] Currently, the Commonwealth is assisting Namibia in creating new laws to protect people's data and prevent cybercrimes from occuring.

Case Study 2: Data Breach at Equifax

With the prevalence of hacking growing more than ever, numerous companies are experiencing data breaches. [30] Data breaches are when information such as personal data is stolen without consent from a certain system or platform.

Hundreds of millions of users' data were stolen in March 2017 from Equifax, an American credit Bureau. [31] People's names, addresses, birth dates, social security numbers, credit card numbers, and other personal information were breached.

[27] Williams. J. (April 13, 2016) *Keys Case Spotlights Flaws of Computer Hacking Law.* Electronic Frontier Foundation. www.eff.org/deeplinks/2016/01/keys-case-spotlights-flaws-computer-hacking-law.

[28] (January 19, 2019) *Proposed UN Cybercrime Treaty Could Undermine Human Rights.* Human Rights Watch. www.hrw.org/news/2021/01/19/proposed-un-cybercrime-treaty-could-undermine-human-rights.

[29] (March 17, 2020) *Commonwealth Helps Countries Make New Cybercrime Laws and Fight Crime Together.* The Commonwealth. thecommonwealth.org/media/news/commonwealth-helps-countries-make-new-cybercrime-laws-and-fight-crime-together.

[30] Muhammad, Z. (February 29, 2020) *Hacking Has Become a Highly Popular Career Choice, Here's Why That's a Good Thing*. Digital Information World. www.digitalinformationworld.com/2020/02/ethical-hacking-is-becoming-a-highly-popular-profession-here-why.html.

[31] Miyashiro. I.K.(April 30, 2021) *Case Study: Equifax Data Breach.* Seven Pillars Institute. sevenpillarsinstitute.org/case-study-equifax-data-breach.

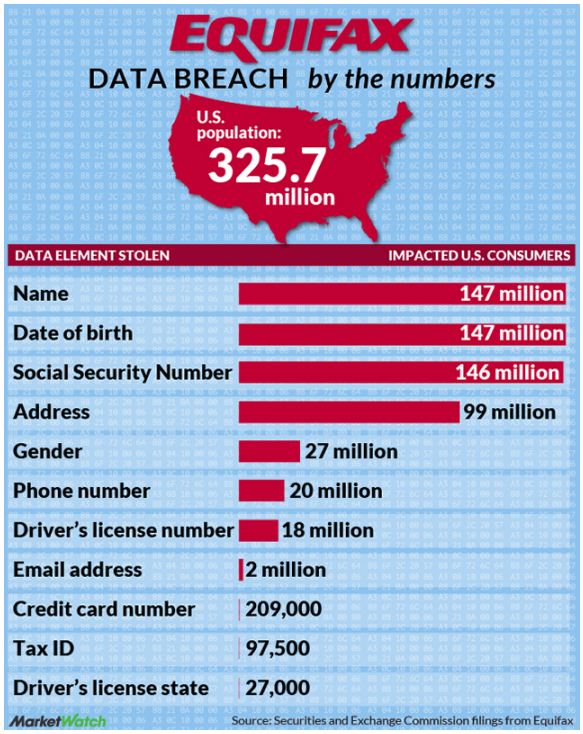

Figure 5: Numbers of impacted consumers [32]

Apache Struts is an "open-source web application framework used for Java EE web applications" [33] which Equifax and many other websites utilized. One issue was that Apache Struts had a vulnerability which was a command injection attack called CVE-2017-5638.[34] On March 9th 2017, Equifax representatives were advised to apply a vulnerability patching to its system which Apache Software Foundation released a few days prior. However, the employee who was in charge of the patching did not comply. When Equifax's IT agency ran scans to identify if there were any vulnerabilities, nothing was out of the ordinary. The scans failed to work.

Because of the lack of security in containing databases, from May through July of 2017, hackers obtained access to Equifax's data. The company published this information more than a month after the attack was discovered. The breach in Equifax was investigated by the FBI, FTC, and the CFPB.[35] Moreover, congressional hearings were held over Equifax's 143 million users' breach. The company faced lawsuits by state and local governments such as the city of San Francisco and Chicago for violating its state policies. [36]

In the U.S., senators Mark R. Warner, Elizabeth Warren, Representatives Elijah

[32] Owen. J.C. (September 10, 2018). *The Equifax data breach, in one chart.*MarketWatch. https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07.
[33] *Apache Struts.* WhiteHat Security Glossary. www.whitehatsec.com/glossary/content/apache-struts
[34] (September 14, 2017) *CVE-2017-5638: The Apache Struts vulnerability explained*Synopsys. https://www.synopsys.com/blogs/software-security/cve-2017-5638-apache-struts-vulnerability-explained/
[35] Fruhlinger. J. (February 12, 2020) *Equifax data breach FAQ: What happened, who was affected, what….* CSO. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.
[36] Miyashiro. I.K. (April 30. 2021) *Case Study: Equifax Data Breach.* Seven Pillars Institute. https://sevenpillarsinstitute.org/case-study-equifax-data-breach/.

Cummings, and Raja Krishnamoorthi reestablished the legislation of holding companies including Equifax accountable for its data breaches. The Data Breach Prevention and Compensation Act enforces strict penalties in which the FTC has to use half of the compensation to consumers. Equifax, under this legislation, would have a total penalty of 1.5 billion dollars. Furthermore, the Office of Cybersecurity was established at the FTC for supervising data breaches.[37]

Through this bill, more accountability will be ensured in order to prevent future data breaches from occurring.

Subtopic II: Cybersecurity in Developing Countries

The Issue

Cyber attacks are a borderless issue, not excluding developing countries. As a result of developing countries rapidly expanding their access to cyberspace, they tend to face "more damage than benefit to both the state and the local economy"[38]. This is particularly difficult for LDCs (Least Developed Countries) which lack fundamental structures, financial stability, human capacity and expertise.[39] Many developing countries face numerous issues other than cyber attacks - it is a pressing goal for Governments to advance their cyberspace for both its citizens safety and its economic growth.

Objectives

The ITU launched "Enhancing Cybersecurity in Least Developed Countries," aiming to ensure LDCs to maximize the economic benefit of ICT in a cybersecure environment.[40]

Case Study: Afghanistan

Afghanistan, a developing country in the middle east, ranked 171st in the GGI (Global Cybersecurity Index. Measures the commitment of countries to cybersecurity) held by the ITU in 2020.[41] There are currently over four million internet users out of its thirty-four million population. Before

---

[37] (May 7, 2019) *Warner, Warren Reintroduce Legislation to Hold Equifax, Other ....* Mark R. Warner. https://www.warner.senate.gov/public/index.cfm/2019/5/warner-warren-reintroduce-legislation-to-hold-equifax-other-credit-reporting-agencies-accountable-for-data-breaches.

[38] Muller. L.P. *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities.* https://core.ac.uk/download/pdf/52116225.pdf

[39] *Enhancing Cybersecurity in Least Developed Countries.* ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CYBLDC.aspx.

[40] *Enhancing Cybersecurity in Least Developed Countries.* ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CYBLDC.aspx.

[41] *Global Cybersecurity Index 2020.* ITU Publications. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

the Taliban regime took over Afghanistan, Russian hacker group Turla is suspected to have targeted the Afghanistan government to take political information. [42] The investigation team found the same malware in the United States and Germany as well. A backdoor, which is "an undocumented way gaining access to the computer system" [43], was installed in the infected machines as an alternative for when the main malware is identified and removed. Despite the close investigation of Afghan's security systems, Turla succeeded in placing this backdoor for almost two years.
We can conclude that data and information are especially vulnerable to theft in developing countries.

Past Actions

2001: **ITU** passed a resolution to combat the misuse of information technologies.
2002: **ITU** passed a resolution to combat the misuse of information technologies.
2003: **ITU** passed a resolution on creation of a global culture of cybersecurity.
2004: **ITU** passed a resolution about creating a global culture of cybersecurity and protecting critical information infrastructures.
2010: **ITU** passed a resolution for creating a global culture of cybersecurity and taking stock of national efforts to protect critical information cybersecurity. [44]

Questions to Consider

- What were the major cyber crimes that have occurred in your country and the measures taken to deal with that?
- What does your country lack in cybersecurity such as financial issues?
- In what ways can your country contribute to global cybersecurity?
- Were there any conflicts that occured due to problems caused by cyber crimes in your country?

Guidelines for Position Papers

Position papers must clearly articulate the current situation of your country and briefly explain the past actions it has taken, further denoting possible solutions. Papers may also include international resolutions and

[42] Luca Bertuzz. *Russian Hackers Targeted Afghan government before Taliban takeover, cybersecurity firm says.* Euractiv. https://www.euractiv.com/section/cybersecurity/news/russian-hackers-targeted-afghan-government-before-taliban-takeover-cybersecurity-firm-says/
[43] *Glossary.* Computer Security Resource Center. https://csrc.nist.gov/glossary/term/backdoor#:~:text=Definition(s)%3A,is%20a%20potential%20security%20risk.
[44] *UN Resolutions* . ITU. https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

strategies to eradicate child labour; however, the main focus **must** be on your country. Every year, a handful of delegates submit position papers with very basic information about their countries, such as geographical location and major trade exports. Unless such information directly relates to the topic, it should not be addressed in position papers at all.

Closing Remarks

Thank you all for taking interest in and participating in JMMUN.
Cybersecurity is a broad topic that applies to all sorts of actors such as the governments, hackers, and victims. It is always important to ask yourself “is this enough?” whenever you are researching about the actions governments or organizations have taken. We hope this experience will benefit you.

Works Cited

About. ITU. www.itu.int/en/about/Pages/default.aspx.

Ekhtyar. H. (August 16, 2017) *Afghanistan: Cyber Crime Code Signed into Law.* Library of Congress. https://www.loc.gov/item/global-legal-monitor/2017-08-16/afghanistan-cyber-crime-code-signed-into-law/ .

Rory. C. (November 17, 2015) *Anonymous Takes on IS*. BBC News. www.bbc.com/news/technology-34850573.

Apache Struts. WhiteHat Security Glossary. www.whitehatsec.com/glossary/content/apache-struts

Buffer overflow. Wikipedia. https://en.wikipedia.org/wiki/Buffer_overflow#History

Miyashiro. I.K.(April 30, 2021) *Case Study: Equifax Data Breach*. Seven Pillars Institute. sevenpillarsinstitute.org/case-study-equifax-data-breach.

(March 17, 2020) *Commonwealth Helps Countries Make New Cybercrime Laws and Fight Crime Together.* The Commonwealth. thecommonwealth.org/media/news/commonwealth-helps-countries-make-new-cybercrime-laws-and-fight-crime-together.

(September 14, 2017) *CVE-2017-5638: The Apache Struts vulnerability explained.*Synopsys. https://www.synopsys.com/blogs/software-security/cve-2017-5638-apache-struts-vulnerability-explained/

Dennis. M.A. (September 19, 2019) *Cybercrime.* Encyclopedia Britannica. https://www.britannica.com/topic/cybercrime.

Muller. L.P. *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities.* https://core.ac.uk/download/pdf/52116225.pdf

Cybersecurity for Business. Invest Northern Ireland. https://www.nibusinessinfo.co.uk/content/reasons-behind-cyber-attacks.

Cybersecurity Glossary of Terms. Global Knowledge. www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/#gref.

Rob. S. (March 16, 2019) *134 Cybersecurity Statistics and Trends for 2021.*Varonis. https://www.varonis.com/blog/cybersecurity-statistics/.

Raymond. P. *Cybersecurity Threats to the COVID-19 Vaccine.* F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/cybersecurity-threats-to-the-covid-19-vaccine.

Cyber Threat and Cyber Threat Actors. Government of Canada. cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

Discover ITU's HISTORY . ITU. https://www.itu.int/en/history/Pages/DiscoverITUsHistory.aspx.

Enhancing Cybersecurity in Least Developed Countries. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CYBLDC.aspx.

Fruhlinger. J. (February 12, 2020) *Equifax data breach FAQ: What happened, who was affected, what….* CSO. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

Smith. G. (December 7, 2017) *FBI Agent: We've Dismantled The Leaders Of Anonymous.* HuffPost. www.huffpost.com/entry/anonymous-arrests-fbi_n_3780980.

Global Cybersecurity Index 2020. ITU Publications. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

Glossary. Computer Security Resource Center. https://csrc.nist.gov/glossary/term/backdoor#:~:text=Definition(s)%3A,is%20a%20potential%20security%20risk.

Muhammad, Z. (February 29, 2020) *Hacking Has Become a Highly Popular Career Choice, Here's Why That's a Good Thing.* Digital Information World. www.digitalinformationworld.com/2020/02/ethical-hacking-is-becoming-a-highly-popular-profession-here-why.html.

Hacktivism 101: A Brief History and Timeline of Notable Incidents - Wiadomości Bezpieczeństwa. Hacktivism 101. www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/hacktivism-101-a-brief-history-of-notable-incidents.

Williams. J. (April 13, 2016) *Keys Case Spotlights Flaws of Computer Hacking Law.* Electronic Frontier Foundation. www.eff.org/deeplinks/2016/01/keys-case-spotlights-flaws-computer-hacking-law.

Our Vision. ITU. www.itu.int/en/about/Pages/vision.aspx.

(January 19, 2019) *Proposed UN Cybercrime Treaty Could Undermine Human Rights.* Human Rights Watch. www.hrw.org/news/2021/01/19/proposed-un-cybercrime-treaty-could-undermine-human-rights.

Ransomware 101. CISA. https://www.cisa.gov/stopransomware/ransomware-101

Owen. J.C. (September 10, 2018). *The Equifax data breach, in one chart.* MarketWatch. https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07.

Malkiewicz, K. (March 8, 2021) *This Year (So Far) in Buffer Overflows.* Dover Micro Systems. https://info.dovermicrosystems.com/blog/2021-buffer-overflows.

UN Resolutions . ITU. https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx.

(May 7, 2019) *Warner, Warren Reintroduce Legislation to Hold Equifax, Other ....* Mark R. Warner. https://www.warner.senate.gov/public/index.cfm/2019/5/warner-warren-reintroduce-legislation-to-hold-equifax-other-credit-reporting-agencies-accountable-for-data-breaches.

What is a DDoS Attack? - Meaning of DDoS. Kaspersky.

https://www.kaspersky.com/resource-center/threats/ddos-attacks

What is a Denial of Service Attack-Palo Alto Networks. Paloalto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

What Is a Threat Actor and Why Should You Care? Sophos Home. home.sophos.com/en-us/security-news/2021/what-is-a-threat-actor.aspx.

What is an IP Address - Definition and Explanation. Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-addres

What is Cyber Espionage? Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

Michael. C. *6 common types of cyber attacks and how to prevent them.* TechTarget. https://searchsecurity.techtarget.com/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them.

15 Facts You Have to Know About Identity Theft. Lifelock. www.lifelock.com/learn-identity-theft-resources-facts-you-have-to-know-about-identity-theft.html.