14th International Conference on Humanities and Social Sciences, 14th ICHiSS 2022
19th May 2022-20 May 2022
Theme:.....

The Factors of the Endless Cyberattacks and Malaysia's Perspective in Securitizing Cyberspace.

Hanis Shaheera
[1]National Defence University of Malaysia

Abstract

The aims of this study are; (1) to investigate the evolving technologies in cyberspace, (2) to explore the human error in contributing to cyberattacks, and, (3) to study the trends of cyberattacks in Malaysia. This research uses a comprehensive literature review under the case study in qualitative research method to study the development of cyberspace which is vulnerable to cyberattacks. The finding of this research demonstrates Malaysia improve its cybersecurity through the creation of the Malaysia Cyber Security Strategy 2020-2024 which is in line with the current context in cyberspace. The initiative taken by the Malaysian government can be adapted to the securitization process. Nevertheless, this study can be used as conceptual research to analyze the challenges of states' boundaries through cyberspace.

Keywords: cyberspace, internet, cyberattacks, government, legislation

1. Introduction

Previously the states engaged in conventional warfare to achieve national objectives; be it to expand territory, obtain resources, or gain more power to influence others. But after the end of the Cold War, the nature of war has changed and added advanced technology which keeps on updating has made cyberwarfare known to be the fifth domain in warfare after the land, sea, air, and space. Nevertheless, last time the states were divided by boundaries, but nowadays the technologies have made the people live in a borderless world where we can get connected through the internet.

According to Dunn Cavelty (2006), since information technology has been popularized with the acceleration in internet users and accepted in the international system, it was somehow exposed to a new set of strategic vulnerabilities (Cavelty, 2010). For example, Operation Desert Storm sparked the idea of cyberwar as it has the possibility of network armies using network communication systems such as radio waves or satellites, hence the decentralized, digital communication systems were a key technology that made network warfare possible (Berkowitz, 2003).

On the other, despite the vulnerabilities in cyberattacks and states being aware of the benefit of cyberspace, the Malaysian government is keen on providing initiatives in introducing internet capability to its people. In 1995, Malaysia entered the internet age, and ever since that the internet users have bloomed. Whilst by the end of 2012, internet users in Malaysia has increased up to 66% of the Malaysian population, which counts for 19 million internet users. Some of the Malaysian government initiatives can be seen through its strategic implementation by introducing IT policy to encourage the internet users

whilst working or use it as part of their daily life, providing public schools with computer labs, tax exemptions for any laptop, and internet connections purchases, whereas the public and private institutions were incorporating in producing experts and graduates in the fields of the Information Technology (IT) (Wok & Mohamed, 2017).

Henceforth, this shows that Malaysia is aware of the contemporary trends of cyberspace and accepts that the world is entering the 4th Industrial Revolution (IR4) despite exposure to cyberattacks. This study intends to analyze the factors of the never-ending cyberattacks and to explore initiatives taken by the Malaysian government in securitizing the issue based on securitization theory.

2. Research Method

This research implements a qualitative method to study in-depth the issue of cyberspace which threatens state security from the perspective of Malaysia. The qualitative research method consists of five approaches which are narrative research, grounded theory, phenomenology, ethnography, and case study. The approach used to conduct research for this study is a case study. Case study research involves the study of a case within a real-life, contemporary context or setting (Yin, 2009). Supported argument by Creswell, a case study is a methodology in which the investigator explores a real-life, contemporary bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in-depth data collection involving multiple sources of information (eg: observations, interviews, audiovisual material, documents, and reports), and reports a case description and case themes.

Therefore, the researcher intends to collect data through secondary sources. The researcher will gather data from books, journals, articles, and reports on cyber statistics, as well as sources from websites, to enrich the information on the factors of the endless cyberattacks. These sources are crucial to strengthen this study and to increase its credibility without neglecting the ethics and manner of managing the sources obtained. In order to overcome some limitations which arose whilst conducting this research, the researcher will apply the triangular method to ensure the credibility of the data obtained.

3. Literature Review

2.1 The Factors of the Endless Cyberattacks

The factors for the endless cyber attacks will be categorized into three aspects; (1) the evolving technologies in cyberspace. (2) the human factors (3) the trends of cyber attacks in Malaysia.

The evolving technology in cyberspace

Technologies nowadays are inseparable from human life. It has made revolutionary advancements; including the introduction of the 5G networks, the Internet of Things (IoT) to Artificial Intelligence, Cloud Technology, and Machine learning; this creates efficiency, reducing costs, borderless communications, time optimization, and offers new opportunities. Therefore, private companies are competing in producing high technologies whilst strengthening their state's influence and power in markets.

According to Riel Miller (1998), societies nowadays are embracing the changing in social, technical, and economic through technologies. The speed, size, and cost are the elements in measuring the technology

revolution at times. Back then, it cost $550,000 to own a megabyte of semiconductors, but today it cost only $4. This phenomenon of technological revolutionary can be described as "*faster, cheaper, and smaller*" (Miller, Michalski, & Stevens, 1998).

On the other, the network technology continues to move forward and delivers greater diversity and higher bandwidth. It could accommodate heavy-duty transmission systems through a fiber optical with rapidity, whilst mobile communications coverage will rain down from a variety of low and high orbit satellites. Hence, the personal network for home installation will be more affordable as it is easy to access and own. Although the communication services may not reach zero cost, it is predicted to be almost to it by three decades of the next century. (Miller, Michalski, & Stevens, 1998).

Meanwhile, the other improvement in technology is Artificial Intelligence (AI). John Pavlus reviews that the AI developments have risen tremendously as it takes about 5 years to dominate the world compared to the evolution of smartphones and the web which takes 10 years and 20 years respectively to *"eat the world"*. Experiencing AI from laboratory curiosity has expanded to the economic sector contributes the most to global GDP in 2017 and 2018 with an estimated $2 trillion (Pavlus, 2019).

This phenomenon of increasing internet users comes from the effort of the Malaysian government. The network technologies have shifted its modernization from the usage of 2G smartphones to 5G smartphones, nevertheless, the affordable value has made it effortlessly owned by most people nowadays. The internet coverage has been improving significantly since the Malaysian cabinet has approved RM21.6 billion to implement the National Fiberisation and Connectivity Plan (NFCP) with the intention to deliver nationwide digital connectivity with robust, pervasive, high-quality, and affordable to all generations. This meets the Malaysian government's objectives to upgrade living standards and come up with new business models with career opportunities (Ying, 2019).

The internet capability and AI technology have shown tremendous advancement by year; so does the development of viruses. The main purpose of the creation of the internet is to connect efficiently, it is not focused on security (Lewis, 2014). According to Nikola Milošević, the first Malware creation back in 1986 by Pakistani brothers, Amjad and Basit was meant to prove that there is no security for using the personal computer (PC). Malware known as Malicious Software is purposely designed to disrupt computer operations, obtain encrypted information, or access the systems of a private corporation (Milošević, 2013).

The internet is known to be an innovation engine, which means it develops faster, and so do the cyber threats evolve speedily than the cyber defense could react. Sophisticatedly, technology has brought so many people to get connected, but at the same time vulnerable to cyberattacks due to the evolution of cyberspace technology. According to FireEye, around 12 million communications between the botnet command and control servers and infected enterprises have been traced back to 2012.

The virus capability instilled by the cybercriminals with two purposes; to gain self-interest and to inflict damage. The attacks usually come in small-scale attacks or large-scale attacks. But the small-scale attack is known to be the most frequently happening in countries. Some examples of small-scale attacks are; spyware, bots and rootkits, spam, phishing attacks, credit card fraud, information theft, corporate information theft, and denial of service extortion. Whereas the large-scale attack includes the denial of service packet floods, exploiting infrastructure components, mass credit card fraud to disable accounts, or damaging clients' systems with widespread botnets (Skoudis, 2009). The large-scale attack could be backed or sponsored by a country and although it may not inflict total damage on its opponent it could still create havoc situations, for example, the Estonian cyberattacks in 2007.

The recent development of Malware is not only applicable for cybercriminals but it is applied by defense forces such as the military, polices, and secret agencies as weapons with the capability to inflict damages without risking human lives. For example, one of the advanced malware computer worms; Stuxnet was reportedly sabotaged and attacked the nuclear program in Iran which caused most of Iran's nuclear centrifuges to be destroyed. The Stuxnet was invented to attack industrial control system which controls nuclear plants and is capable to remain hidden from detection (Kerr, Rollins, & Theohary, 2010).

The Human-Error factors

Countries could have the most sophisticated technology in the world, but still face the same problem of human error which contributes to incompetent outcomes and leads to cyberattacks. According to Datuk Dr. Amirudin Abdul Wahab, 99% of cyberattacks come from the human error factor in Malaysia, thus the safety of Malaysian cyberspace should not be depended on alone on the best technology. In 2018, Malaysia has recorded around 2907 cases of fraud, out of 5078 cases of cyberattacks. The fraud cases were reported to be the highest and Datuk Dr. Amirudin Abdul Wahab claimed that *"most scams are about money and this is why humans are the weakest when it comes to money"* (Othman, 2018).

Research conducted by Inthrani Shammugam, et al, explains that the top three threats in information systems come from technical threats, followed by social engineering and deliberate human threats. Thus human error has become a critical challenge that has been continuously faced by everyone. The factors for this to happen are due to weak and inadequate ICT security policies or procedures, lack of preventive measures, failure in implementing risk assessment on ICT assets, and lack of enforcement of ICT security compliances and audits (Shammugam & et al, 2021).

According to Deursen, he describes a wide range of human errors that expose information systems including improper system configuration and deficient management of security patches, poor authentication procedures including use of default user ID and passwords, weak passwords, sharing passwords, physically losing devices with protected data on them, staying logged in when leaving accessible computers unattended, accessing unsafe websites and opening unsafe emails, and inadvertent sharing of confidential data by sending it to the wrong email address (Deursen, 2015).

Therefore, human error is known to be an endless issue as Armerding cites a report that indicates 56% of workers who use the Internet whilst working receive no security training at all (Coffey, 2017). Without appropriate exposure to workers regarding the use of information systems, despite the ability of organizations in using strong technological security procedures still often pay insufficient attention to human sources of vulnerabilities. Hence it strongly advocates for enhanced security training (Howarth, 2014).

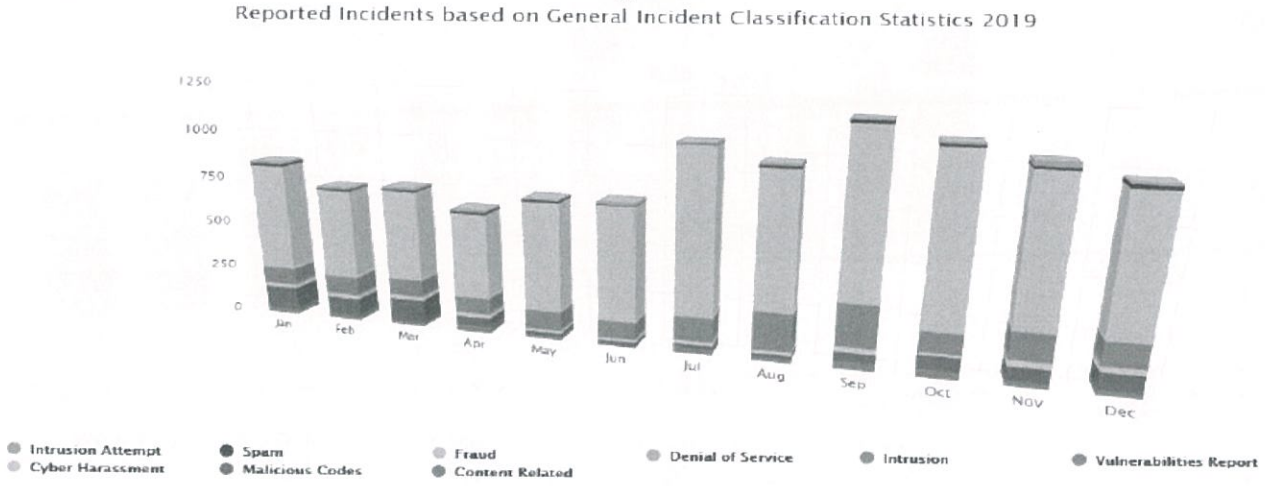
Whilst human error contributes to the cyberattacks in Malaysia, the next topic will discuss the cyberattacks trends which happen in Malaysia and the types of cyberattacks that frequently happen.

The cyberattacks in Malaysia.

The type of cyberattacks could be on a large scale which causes the entire nation to be disrupted in cyberspace, or the small-scale cyberattacks with small impact, mostly happen due to profit-making purposes. According to MyCert Report Statistics from 2018 to August 2021, most of the cyberattacks happened due to Fraud, whilst the second higher cyberattacks come from Intrusion. And this is followed by Malicious Codes, Intrusion Attempt, Spam, Denial-of-Sevice, Vulnerabilities Report, Content Related,

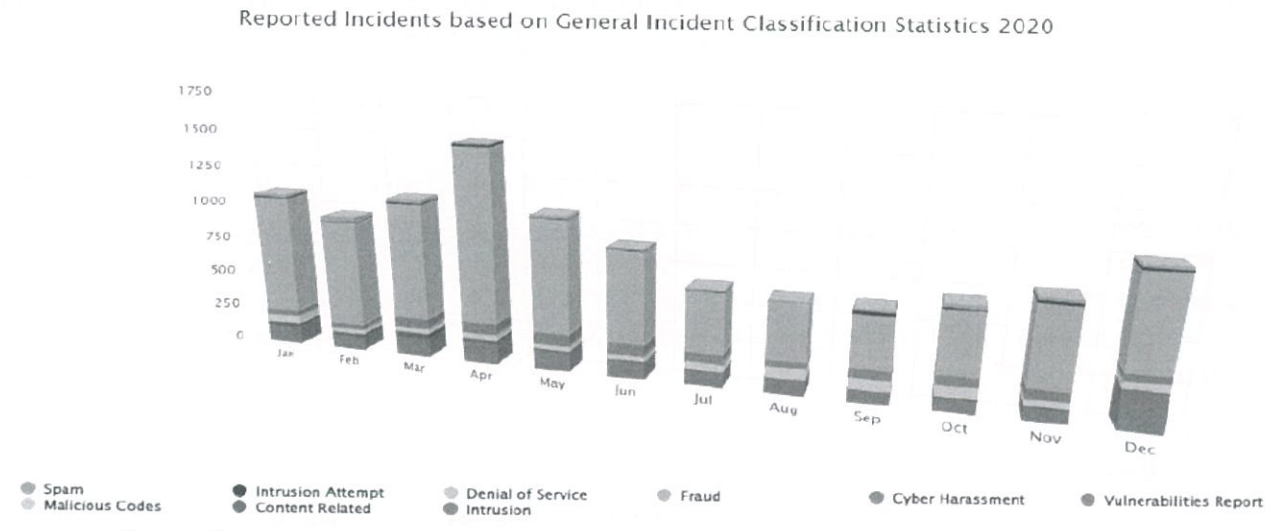
and Cyber Harassment. Total reported cyberattack incidents in 2018 was 10,699, whilst in 2019 was 10,772, followed by 2020 reported 10,790, and in 2021 until August incident reported was 7,495 (Malaysia, n.d.). The statistics from 2018 until August 2021 show the total cyberattacks reported have gradually increased. The statistics of cyber trends in Malaysia can be referred to in Figure 1, Figure 2, and Figure 3. This makes cyberspace is still vulnerable to threats since the total cyberattacks have not resolved yet.

Figure 1.



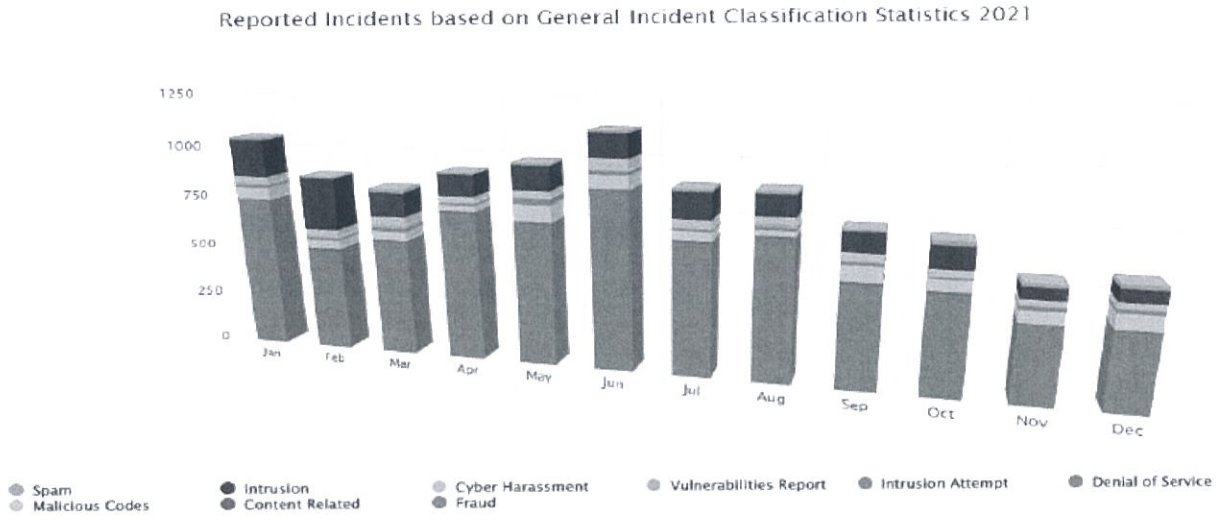
Source: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=0d39dd96-835b-44c7-b710-139e560f6ae0

Figure 2.



Source: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2650ed29-88be-4cec-86cc-13f8e07ae228

Figure 3.



Source: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=77be547e-7a17-444b-9698-8c267427936c

Trends of cyberattacks in Malaysia has not decreased might be due to factor of increasing in online activities. Since 2019, the international phenomenon has change which the pandemic Covid-19 has affect worldwide. This cause the government to implement policy of Movement Control Order (MCO) to curb the Covid-19 virus from spreading. Hence all of the activities has change from physical activities such as working in office to online activities, such as working from home. This has effect on e-commerce as well. The usage of e-commerce has increased as it push the traditional retail merchants to adapt to the new environment of e-commerce; and it is accepted by most countries.

On the other way, the results of Fraud attacks during the pandemic have arose significantly where the global network found that the rate of account takeovers (ATO) has increased up to 400% on e-commerce during the pandemic. These happen due to data breaches in which consumer credentials are stolen, combined with the fact that over 65% of users recycle the same password across multiple platforms. Cyberattackers usually launch cyber attacks such as phishing with the email address of targeted victims (Henriquez, 2021).

4. Findings

The use of cyberspace provides not only advantages but also disadvantages. The government plays a crucial role in ensuring its national security is secured and anything which brings harm to the nation shall be forfended. The researcher has elaborate on the causes of the endless cyberattacks, hence this section intends to explore the Malaysian government initiatives in mitigating cyberattacks.

Referring to Copenhagen School, a securitization model was developed to explain the process of a state in perceiving any threats which could harm the state, and the role plays by the decision-maker in securitizing the object through speech act. Hence the process of securitization includes the issue area, securitizing actors, security concept, the process of securitization, the first outcome of the degree of

securitization, and the second outcome consisting of the impact on the threat, and lastly the conditions affecting securitization (Caballero-Anthony, 2016).

Referring to Securitization theory, the issue area can be referred to in cyberspace as concurrence as an object of existential threat among society and government sectors. The securitizing actor or the Malaysian government needs to address the cyberspace issue because it is the authority of the government was the one who introduced the internet technology to its country, hence it is its responsibility to ensure the internet security to its people, or else It would bring harm towards its country in return. If it looks at the sovereignty, the country should protect its border and its sovereignty, however, the character of cyberspace hence is borderless, all the data and information could cross the countries in a short period of time and some information might contain threats and other harmful purposes.

Under the security concept, cyberspace could pose threats at all levels of individuals, state, and international levels. Cyberspace technology has challenged the Peace of Westphalia in 1648. This shows the environment changes, hence the policy should too. Peace of Westphalia has been signed by the European countries to end the war and to recognize the state's border and the government shall have rights towards its own border. But with cyberspace coming in with its purpose to ease the flow of information by using satellite and undersea cable, it might not harm the state's border physically but the flow of information without having to travel does bring harm especially when it contains threats or any bad intention.

On the other, the process involves the use of speech acts to convince the audience regarding threats that exist. The decision-maker usually applies politics, influence, or even manipulation in order to ensure it serves the interests. The role of the decision-maker in convincing the people regarding cyber threats is crucial because these cyber threats come from small scale and large scale. The small scale usually impacts personally, with money-oriented, defame, or misuse information. Whereas the large scale usually comes with big agenda towards the government such as the use of propaganda, to gain more influence and followers for the left-wing party, to attack by using the Distribute Denial of Service (DDOS) towards the authorized personnel and cause jammed and blocking from getting the right information, hence the impact can be seen from inside the country, it could cause chaos inside the country and the attacker could launch the attack somewhere far by using a personal device.

From the Malaysian government's perspective, the government has come up with initiatives in strengthening and combating cyber threats from top-down management, and with the establishment of the National Cyber Security Agency (NACSA) in supporting Malaysia's national security and serving as a response to cyber security threats. Other initiatives include collaborating with private sectors in providing better cooperation in mitigating cyber threats, creating awareness to the public in surfing the internet and practice safe conduct in cyberspace, updating cyberspace legislative and regulatory framework in combating cyber threats, and introducing the "Malaysia Cyber Security Strategy 2020-2024". Six principles were outlined to support the National Cyber Crisis Management namely; readiness program, national cyber crisis management structure, national cyber-threat levels, Computer Emergency Response Team (CERT), cyber security protection mechanism, and response, communication, and coordination procedures (Council, 2020).

5. Conclusion

In a nut shell, states and the international system plays an important role in regarding the cyberspace secure and how these cyberattackers adapt to new strategy. With the current internet connection of 5G and most of the develop and developing countries are started to adapt it, whilst at the same time the current situation of pandemic Covid-19 has caused a major shift and flows of the internet using among people has increased the vulnerability or exposure to cyber threats.

The technology keeps changing and improving, and so does its threat. The cyberattack will use this opportunity to adapt to the new technology and find its way to infiltrate and exploit for their own interests. The effect of a cyberattack might not be fully blown up the whole nation, but the ability of the cyber attacker to instill fear among the people is enough to pressure the government to work or improve its policy in securing its cyberspace. Hence the government is the one who brings the internet to its people, yet it should be the government to implement an effective policy to secure the policy for its people as consumers to use it. And it is best if the government could cooperate with the private sector in producing the best strategy for adapting to the cyberspace environment.

References

Berkowitz, B. (2003). *The New Face of War: How War will be Fought in the 21st Century.* New York: The Free Press.

Caballero-Anthony, M. (2016). *An Introduction to Non-Traditional Security Studies.* Singapore: SAGE.

Cavelty, M. D. (2010). Cyberthreats. In M. D. Cavelty, & V. Mauer, *The Routledge Handbook of Security Studies* (pp. 180-189). London: Routledge.

Coffey, J. W. (2017). Ameliorating Sources of Human Error in Cybersecurity: Technological and Human-Centered Approaches. *8th International Multi-Conference on Complexity, Informatics and Cybernetics (IMCIC 2017)*, (p. 86). Florida.

Council, N. S. (2020). *Malaysia Cyber Security Strategy.* Putrajaya: National Security Council.

Deursen, N. v. (2015, Jan 13). *How to Reduce Human Error in Information Security Incidents*. Retrieved from Security Intelligence : https://securityintelligence.com/how-to-reduce-human-error-in-information-security-incidents/

Henriquez, M. (2021, March 31). *5 minutes with Jane Lee: The fraud supply chain, cyberattacks and more*. Retrieved from Security Magazine: https://www.securitymagazine.com/articles/94927-minutes-with-jane-lee---the-fraud-supply-chain-cyberattacks-and-more

Howarth, F. (2014, Sept 02). *The Role of Human Error in Successful Security Attacks*. Retrieved from Security Intelligence: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010). The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. *Congressional Research Service*, 3.

Lewis, J. A. (2014, March). *Cyber Threats and Response: Combating Advanced Attacks and Cyber Espionage.* Washington DC: Center for Strategic and International Studies. Retrieved from Center for Strategic and International Studies: https://www.csis.org/analysis/cyber-threat-and-response

Malaysia, C. (n.d.). *Incident Statistics*. Retrieved from MyCert Malaysia: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=e49c91c1-4b04-4748-8152-294764f9c8dc

Miller, R., Michalski, W., & Stevens, B. (1998). *The Promises and Perils of 21st Century Technology: An Overview of the Issues.* France: OECD.

Milošević, N. (2013). History of Malware. *Computer Security*, 1.

Othman, N. Z. (2018, Oct 29). *Towards a Safer Cyberspace: Most 'Attacks' due to Human Error*. Retrieved from New Straits Times: https://www.nst.com.my/lifestyle/bots/2018/10/426298/towards-safer-cyberspace-most-attacks-due-human-error

Pavlus, J. (2019, March 12). *AI is moving too fast, and that's a good thing*. Retrieved from Fast Company: https://www.fastcompany.com/90429993/ai-is-moving-too-fast-and-thats-a-good-thing

Shammugam, I., & et al. (2021). Information Security Threats Encountered by Malaysian Public Sector Data Centers. *Indonesian Journal of Electrical Engineering and Computer Science*, 1826.

Skoudis, E. (2009). Information Security Issues in Cyberspace. In S. H. F. D. Kramer, *Cyberpower and National Security* (pp. 172-187). Washington DC: National Defense University Press.

Wok, S., & Mohamed, S. (2017). Internet and Social Media in Malaysia: Development, Challenges and Potentials. *The Evolution od Media Communication*, 47.

Ying, T. X. (2019, August 28). *Cabinet okays RM21.6b plan to give Malaysians faster and better Internet.* Retrieved from The Edge Markets: https://www.theedgemarkets.com/article/cabinet-approves-rm216b-national-connectivity-plan