e-Bangi Faculty of Social Sciences and Humanities Universiti Kebangsaan Malaysia
Journal of Social Sciences and Humanities

eISSN: 1823-884x

Volume 21, Issue 2, DOI: https://doi.org/10.17576/ebangi.2024.2102.17

Article

Cyber Security Crisis/Threat: Analysis of Malaysia National Security Council (NSC) Involvement Through the Perceptions of Government, Private and People Based on the 3P Model

Siti Sabrina Imji Rahim*, Mohd Ikbal Mohd Huda, Shahrizal Sa'ad & Ravichandran Moorthy

Centre For History, Politics, and International Affairs, Faculty of Social Sciences & Humanities, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia

*Corresponding Author: teenasabrina@gmail.com

Received: 20 February 2024
Accepted: 28 May 2024

Abstract: The new crisis/threat namely cyber security has become a priority for Malaysia due to the huge impact not only on this country, but also the people. Malaysia shows a trend of increasing cyber security despite various initiatives taken by the government to deal with it. The government has established the National Cyber Security Agency (NACSA) under the auspices of the National Security Council (NSC) where NACSA acts to coordinate all forms of cyber management with other agencies that handle cyber in Malaysia. The question arises is why cyber security continues to increase which is necessary to analyze to what extent NSC as a coordinating agency for managing cyber security successfully plays its role. The study carried out by analyzing the perception of the government, the private sector, and the people on the effectiveness of NSC 's involvement based on the 3P Model via qualitative methods that refer to primary and secondary documents such as official reports, academic journals, and online news as well as through interviews with government officials involved. The results of the analysis found that NSC's involvement is proactive in dealing with cyber security. NSC's coordination with other agencies is active, but there are challenges that need to be addressed. Coordination between the central and state NSC is effective. Political interference has influenced the determined decision but minimal. Cyber security management has led NACSA/NSC to updating/drafting the laws, increased program/strategy, more prominent, and collaborative involvement of all parties.

Keywords: Cyber Security crisis/threat; NACSA; NSC; perception; 3P Model

Introduction

Cyber security is one of the crises or threats to national security, where if it is not prevented, it can affect not only national security, but also the people and the national economy. Referring to NSC Directive No. 26, cyber threat means a threat that originates from the Internet or a network using a data communication path that affects the confidentiality, integrity and availability of information systems from within an organization or from a distance as well as the dissemination of information through a cyber medium that is contrary to national laws and capable of threaten national security.

Along with the desire to make Malaysia a developed country and a hub for digital economic development, the Malaysian Government has placed a high commitment in the use of information and communication technology (ICT) as a driver of national and socioeconomic development. However, the increasing dependence on ICT and the Internet has opened up space for cyber threats. Accordingly, the protection of the country's cyber space needs to be prioritized and managed through organized and clear cyber security management (NSC Directive No. 26). Especially now Malaysia is showing an increasing trend in

cyber security. Records also show that Malaysia hit 57.8 million virus attacks in the first quarter of 2022, which accounted for 1.14 percent of the total number of cyber security worldwide (Bernama, 2022).

If we look to foreign countries, cyber security at China have become aggressive, silent, sophisticated and disruptive (Lai & Rahman, 2012). In the case of United States (US), cyber security issue has handled more structured and holistic approach, led cyber security issues in the US have proven to be addressable where previously failed (Lilli, 2020). In United Kingdom (UK), cyber threats require cooperation from other countries and a strong agreement (Stevens & O'Brien, 2019). UK perform cyber security cooperation with Japan where since 2013, both countries are in a good position on cyber security (Matsubara, 2014). For the India government, cyber security is only effective with a leading role by the private sector (Medcalf, 2017).

In Canada, cyber security threat has been address through international relations cooperation and social domestic forms of control (Zajko, 2015). In Australia, the government has addresses cyber threat by modeling the initial response from outside such as US (Smith & Ingram, 2017). In New Zealand, this small country faces several challenges in improving its national cyber security related to resources and dilemma between maintaining security and the freedom of people (Burton, 2013). In Finland, among the measures taken to deal with cyber security is through the government's by creating a Security Strategy Cyber Finland (Lehto & Limnell, 2020).

Along with what is happening in foreign countries, in Malaysia, communication and mobile technology that acts as a facilitator for administrative, business and social affairs is also exploited by criminals and malicious parties. These groups carry out their activities by manipulating the borderless and anonymous cyber space. This situation become more complex and challenging with the transition of technology to the era of Internet of Things (IoT) and Industrial Revolution 4.0 (IR 4.0) which is able to connect various equipment and hardware in the cyber environment. This development open up space to increasingly complex and unpredictable cyber threats. The country face huge implications due to the risk of this threat, if not managed effectively (NSC Directive No. 26).

Based on the research by these past scholars and NSC Directive, cyber security crisis/threat has attacked both Malaysia and foreign countries which it become the countries main concern where in foreign countries, various initiative have been taken into place and bring benefits to the countries, also lead to country good, assist to faced the challenges and managed to curb the cyber threat. Therefore, it is very important for a study to be carried out to see how Malaysia deals with cyber security, the responsible institution and the level of effectiveness, as well as the status of whether it is able to reduce cyber security threats or otherwise. There are many previous studies conducted about the cyber security issues, but none of them have focused on the main institutions that deal with it (NSC). Institutional review is important due to the effectiveness in dealing with cyber security threats is closely related to institutional integrity. Besides, there is also ignorance and confusion about which institution is primarily responsible for coordinating issues related to cyber security.

Literature Review

1. Malaysia Cyber Security

In Malaysia, cyber security crises/threats are handled and coordinated by the NSC. NSC has established NACSA to deal with all forms of cyber crises/threats. Hence, this article analyze Malaysia NSC's involvement in dealing with the cyber security. This analysis allows NSC's effectiveness in dealing with this crisis/threat to be unraveled. At the same time, this article can also show the impact of the cyber security crisis/threat on the national security management structure managed by the NSC, as well as being able to assess the level of NSC coordination with other security agencies, also central and state NSC in dealing with these crisis/threat. Finally, the analysis can also identify the political interference effect on the effectiveness of cyber security crisis/threat management by NSC and other security agencies.

To date, cyber security indeed increasing involving losses up to RM500 million a year based on reported cases and bank attack that causes disruption of bank services/systems. One of victims also involved the Bank Manager with total loss of RM200,000 (Md. Zain, S. N, personal communication, January 24, 2023). The Chief Executive Officer of Cyber Security Malaysia (CSM), Amirudin Abdul Wahab, classified cyber security into nine categories namely spam, attempted intrusion, denial of service, fraud, cyber

interference, vulnerability reports, malicious code, content-related and intrusion. According to him, a total of 3,647 cyber security incident reports were received during the first four months of 2021 and the previous year are 10,790 cases in 2020, 10,772 cases in 2019, 10,699 cases in 2018 and 6,926 cases in 2017 (NSC Official Website, 2022).

Mat et al. (2020) stated that the cyber security incidence in Malaysia is increasing, along with the increase in the use of the Internet by all levels of society. Weaknesses in existing systems and governance also cause the threat increment. Countries face challenges from international criminal organizations that abuse platforms and access to the Internet for illegal cross-border activities. Cyber security has become a serious economic concern in Malaysia. Their statement is supported by Bansal (2018) who stated that the number of cyber security in Malaysia is increasing at an alarming rate. Supayah and Ibrahim (2016) mentioned that although the Malaysian government takes various measures to control and protect its citizens, cyber security is increasing along with the number of cyberspace users.

Malaysians' awareness of cyber security is still low and many do not practice methods or procedures for using technology and Internet in a positive, ethical and responsible manner. This can be seen through the number of cyber security incidents in Malaysia that continue to increase, seeing netizens become victims of various types of cyber security incidents. Therefore, Malaysians need to be expose through cyber security education and awareness programs from time to time (Berita Harian, 2021). Harib et al. (2017) stated that citizens are aware of the risk of cyber security, but they do not take action to protect themselves from being attacked. This statement is supported by the study of Zulkifli et al. (2020) which showed that most Malaysians are aware of cyber, threats and risks of being in cyberspace, but very few of them take security measures when operating online.

Zahri et al. (2017) stated that young Malaysians are well exposed to the use of Internet from a very young age, with device ownership starting as early as the age of seven. They stated that monitoring should be done more often and modules should also be developed at the school level for early exposure. Education will help ensure a good cyber attitude among young people in Malaysia. His statement is supported by Omar et al. (2021) who stated that there is still a lack of information security awareness among youth.

Based on these past scholars studies analysis, it showed that NACSA need to enhance their strategic ways especially in educating and raise awareness among young people about the importance of cyber security. For this purpose, it is very important for the NSC to involve the people as well as the private sector in deciding on the strategy related to cyber security. This matter can indirectly increase the level of people awareness.

2. Theoretical Framework

Hence, researchers have developed the Tripartite Model of National Security (3P Model). This model involves three (3) actors namely the government, the private sector, and the people. The researchers applied this model due to the importance in involving the whole of government (WOG) and whole of society (WOS), in which the awareness of cyber dangers can be increased, and people also feel that the government considered and listens to them. This is in line with what is stated in the National Security Policy 2021-2025 regarding "security is a shared responsibility". Besides, it can also help the study to get the whole perception of NSC effectiveness level.

The background of this model was developed based on the combined writings of past scholars namely Park and Chung (2021), Zaini (2020) and Ite (2003). How it is combined is that Park and Chung (2021) have found that cooperation between the government and the private sector in curbing the Covid-19 Pandemic in South Korea has caused the spread of this pandemic to be stopped in just one month. Zaini (2020) on the other hand found that cooperation between the government and the public (channeling information from the public to the government) has succeeded in defeating the human smuggling syndicate at the Malaysia-Indonesia border.

Finally, Ite (2003) found that the firm commitment between the Nigerian government in dealing with the issue of people's poverty by showing a trustworthy attitude has increased wealth and economic development. Therefore, based on the writings of these three scholars, it is concluded that cooperation between the government and the government, the government and the private sector and the government and

the people have been able to deal with security threats and balance the national economy. The diagram of the 3P Model is as Figure 1 below. Thus, this model can reflect the views of all parties on a national security issue to get a fair sight. It is very important for the government to take into account the people's ideas and suggestions on how best to deal with cyber security. This model can then be used by other future writers to assess the level of a security issue and the effectiveness in dealing with it.

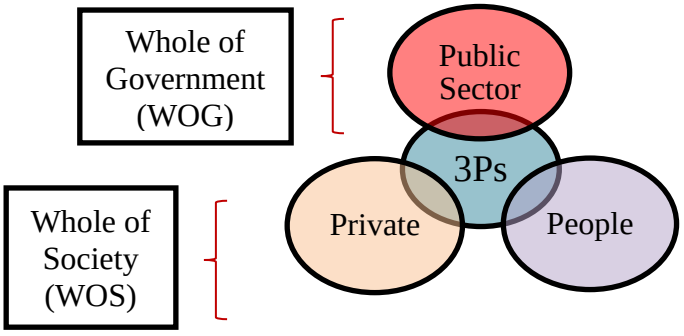

Figure 1. Diagram of the Tripartite Model of National Security (3P Model)
Source: Developed by Author's based on the ideas from Park and Chung (2021), Zaini (2020) and Ite (2003)

Methodology

1. Research Design

This study uses a qualitative method which is a research method through search, description, and non-numerical observation. This method provides information, interpretation or meaning in a communication process as well as about human nature and condition by using a general view of any social action (Hamzah, 2004). Qualitative data collection methods commonly used are observation, interview, and document analysis (Jasmi, 2012). For this study, data is collected through interview and document analysis.

2. Data Collection Process

Interviews have been conducted with senior government officials from the NSC namely Rodzi Md Saad (former Director General of National Security), Hamzah bin Ishak (Deputy Director General of National Security), Zahari bin Alias (former Deputy Director General of National Security), Md. Shah Nuri bin Md. Zain (former Director of NACSA) and Rohayu binti Hussin (former Assistant Director, Border Cooperation Section, Land Border Management Division, NSC, who is also a MINDEF navy that attached in NSC as focal point).

Also, with one of Ministry of Home Affairs (MOHA) senior government officer, Sara Leonie Aloysious Tamor. The informants selected from the NSC are heads of departments and divisions who have been working at the NSC for a long time, reaching almost 30 years. Therefore, they have extensive experience in handling issues related to national security, including cyber security. The selected senior MOHA official is also due to her experiences in managing strategic security management and has a high level of experience.

Document analysis is collected through the division of primary data and secondary data. Primary data is obtained from NSC official government reports such as directive and policy paper, while secondary data is from academic journals/articles/thesis and online news namely Bernama, Berita Harian, MyMetro and Astro Awani. The data collection conducted have been approved by the Ethics Committee of the National University of Malaysia.

3. Analysis Data

Data were analyzed through 3P model on the perception of the government, the private sector and the people in issues related to cyber security. In this regards, the government's perception of cyber security issues including the challenges and effectiveness in dealing with them were analyzed through interviews and document analysis, while the perception of the people and the private sector on the same matter were analyzed through document analysis solely.

Finding

1. People and Private Sector Perception

From people and private sector perception, the Senior Vice Chairman of the Malaysian Crime Prevention Foundation, Lee Lam Thye, stated that if cyber security is not dealt with collectively, it has the potential to create a major impact in various aspects and is capable of threatening the country harmony and security including threatening religious and racial aspects, thereby affecting the people unity. He hope that the government takes a holistic approach and adaptation in terms of human resources, processes and technology in dealing with cyber security (Rosli, 2020).

Selvakumar Manickam, Science University of Malaysia, said data leaks had always be one of major security issues worldwide. He is on the view that the government should ensure all systems and software are kept updated and with the latest security patches, train network engineers and system administrators to gain the security-related skills to manage and configure systems securely, also hiring cybersecurity experts to stress-test the government systems to proactively identify weaknesses/vulnerabilities and remedy them. He also suggested that all government staff should be systematically educated to ensure they do not become the victim or a conduit to the cybercriminals (Krishnan, 2021).

Mohd Daud and Mohd Yusof (2022) stated that the law enforcement weaknesses and the lack of public awareness are also among the factors on the increase in cyber security, where need measures to emphasize community awareness, especially netizens on social media who are vulnerable to cyber security. They stated that public-private cooperation in the fight against cyber security can increase the security aspect to a higher level. They also suggested the government to introduce new laws on punishment.

The Central Bank of Malaysia (BNM) Manager (Inquiries and Complaints Division), Vijayadurai Singgatore stated that BNM continuously urges the public to be aware of tricks or offers made by scammers and to be wise in using technology, as well as be careful in using applications in media social. He stated that the banking industry always improving the security level. AmBank Islamic chief executive officer, Eqhwan Mokhzanee Muhammad urged that when customers suspect they have been scammed, they should immediately contact the bank's customer service line (Bernama, 2022).

The Vice-Chancellor of the National Defense University of Malaysia (UPNM), Hasagaya Abdullah stated that cyber security threats are seen as a serious issue with a frequency and intensity that grows every year where no country is spared from threats that also affect the economy, defense, military and security domain. Therefore, he is of the view that the country needs to formulate strategies and initiatives for more comprehensive preparation in addition to strengthening the entire cyber security machinery to face emerging challenges and there needs to be greater cooperation at the international level (Bahaudin & Haqimi, 2022).

2. Government's Perception

From the government's perception, Rodzi Md Saad, the former Director General of National Security stated in interview session that new threats such as cyber securitys appear with the advancement of information technology. It also happens if the community is not aware and gives space. The government, the private sector and the people cannot escape from the need to use online facilities. However, we are not aware that it can lead to the issue of information leakage due to intrusion. He stated that NSC dealt with it through NSC Directive No. 26. National preparedness to deal with cyber threats cannot be faced alone and must be together for the sake of mutual success (Md Saad, R, personal communication, July 14, 2022).

According to interview with Hamzah bin Ishak, Deputy Director General of National Security (Security Management), he mentioned that security issues such as cyber security now demand that NSC's role to be publicized. Thus, NSC which used to act behind the scenes has become more prominent through increased communication for all parties to jointly look out of national security. However, the level of secrecy must still be maintained, where i.e the information shared to the public and media is on basic term only to allay the public's fear but for tactical issues remain in coordination between the security agencies and the relevant parties (Ishak, H, personal communication, July 18, 2022).

Zamri Misman, the former Deputy Director General of National Security (Strategic Security) stated that NSC found an increase in the threat of cyber security and a few series of attacks were detected throughout

2022 by threat groups, linked to certain countries. He also stated that the threat from the organizations network is expected to occur continuously, parallel to the current country geopolitical development. Therefore, he suggested that all government and private organizations consistently strengthen network security defenses, also organizations build capacity and implement continuous training that gives priority to improving the skills and abilities of ICT security officers (Ismail, 2022).

Zahari bin Alias, the former Deputy Director General of National Security stated in his interview that cyber crisis/threat is still under control but has not been fully resolved such as issues related to scammers. He is also of the view that the government, the private sector, and the people still do not have a high awareness of cyber security. He stated that NACSA acted to coordinate policy and CSM as an implementer in managing cyber security. He saw that there was good coordination between NACSA and CSM, but now they are seen as competing in functions and roles. According to him, from the aspect of coordination between the central NSC and the state NSC related to cyber security, cyber is largely managed by the central NSC. He also stated that there is political interference that has an impact on the cyber security management by NSC due to political membership present in NSC Session (Alias, Z, personal communication, July 14, 2022).

For the level of NSC coordination with other security agencies in handling cyber security, Shah Nuri bin Md. Zain, former Director of NACSA, said in his interview that national security management in Malaysia Cyber Security Strategy (MCSS) 2020-2024 supports NSP. Security supports policies such as maritime cyber security, borders, and others. Security also involves intelligence. NACSA provides intelligent information to the agencies from the information obtained. The intelligence information provided has a triangle and several layers including NACSA, NSC, Malaysian Armed Forces (MAF) enforcement and Royal Malaysia Police (RMP). Cyber security is involved with all Ministries of social, religious, national development and all using a digital framework. Therefore, cyber security risks do exist. If there is no safety element, it is riskier (Md. Zain, S. N, personal communication, January 24, 2023).

According to Shah Nuri, there is no issue of sharing cyber information, but only related to companies from other countries who reluctant to share when faced with a cyber security due to worried about their company's reputation being damaged even though NACSA will not divulge the secrets. NACSA aim is to provide/share advice and initial steps to address it. Therefore, NACSA has proposed to enact a new law that obliges companies and agencies to share information with NACSA but received opposition from some parties. NACSA needs to be an enforcement agency so that companies and agencies can report to NACSA and NACSA can access their systems to be used as evidence. This requires NACSA to carry out a study. Countries such as Singapore and Thailand have also implemented it (Md. Zain, S. N, personal communication, January 24, 2023).

As for the level of effectiveness in the central NSC and state NSC coordination when dealing with cyber security, Shah Nuri is of the view that when MCSS is implemented, at the same time NSC launches NSP. Therefore, NACSA coordinates in each state to have an officer with knowledge in the field of cyber security where NASCA provides training, as a focal point at the state level. Previously, it was only managed by the central. From the effect of political interference on the effectiveness of cyber security management by NACSA, he stated that political interference is very minimal and there is no reason for interference (Md. Zain, S. N, personal communication, January 24, 2023).

Then Shah Nuri stated that knowledge must be present when dealing with industry because the industry belongs to those who are mostly intelligent. He once held a meeting through a breakfast activity together with the bank’s CEOs in Malaysia. There needs to be an understanding of engagement because if they agree, it can be implemented efficiently. Thus, there is also the need to have leaders with strong characters. In addition, as a coordinating agency, Shah Nuri thinks that it is necessary to think about how to enable private companies to cooperate with the government. Other countries also experience this problem. However, due to NACSA under NSC, enables it to coordinate and gain support cooperation from industry and private companies, as well as having expertise (Md. Zain, S. N, personal communication, January 24, 2023).

According to an interview with Sara Leonie Aloysious Tamor, Chief Assistant Secretary, MOHA, she stated that NSC is proactive in dealing with cyber security crises/threats through NACSA. She also mentioned that there is also a special section that handles cyber security issues in MOHA (Tamor, S. L, personal communication, July 14, 2022). Then an interview with Rohayu binti Hussin, former Assistant Director

(Senior), NSC, who is also a MINDEF navy seconded to NSC, stated that at MAF, there is a cyber security section that conducts monitoring at MINDEF (Hussin, R, personal communication, July 14, 2022).

The Malaysia Prime Minister in 2019, Muhyiddin Yassin, stated that cyber security should be the priority of every country, especially in matters that underlie the economy and national security. He stated that cyber security has become an issue and any country will not be able to deal with this problem alone due to cyber threats knowing no borders and becoming more sophisticated and complicated. According to him, the government has implemented MyDigital Initiative through NACSA to encourage all Malaysians venture into digitization and seize the opportunity to improve living standards, reflecting the government's commitment towards efforts to improve national defense in protecting the cyberspace environment. All action plans under the MCSS 2020-2024 were aligned with the MyDigital initiative as an essential element to achieve the vision of providing a safe, secure and resilient cyberspace. MCSS has also outlined 113 programs under its 35 action plans, and one of them is to hold a bi-annual international conference and exhibition, also known as CYDES (BH Online, 2021).

The Deputy Prime Minister in 2019, Wan Azizah Wan Ismail stated that NACSA issue a National Cyber Security Strategy in 2019 to deal with cyber threats comprehensively. According to her, this strategy is implemented through the mobilization of energy resources and infrastructure development that focuses on the formation of a National Cyber Security Workforce to ensure that the country can optimize the use of existing resources (Hasnan, 2019).

The MCMM Minister, Saifuddin Abdullah, stated that RM1.8 billion has been allocated to implement the Cyber Security Strategy program 2020-2024, where this initiative is provided by NSC to empower CSM and NACSA. According to him, the approach implemented by the government is to deal with the issue of cyber security, for instance Macau Scam with comprehensive approach. He also stated that the government has detected more than 1 million prepaid phone numbers registered suspiciously until October 2020, of which more than 920,000 have been terminated while more than 400,000 have also been updated and confirmed safe for use (Suhaimi, 2020).

Discussion

All above being said, in NACSA's handling the cyber crisis/threats, literally there is an inherent weakness which NACSA still need to improve their services that cause by the confusion and ignorance in the function of managing cyber threats where people think that NACSA is under the Ministry of Communications and Multimedia Malaysia (MCMM) and not under NSC. It stems from the lack of awareness activities about the functions and roles of government agencies to the public (Tamor, S. L, personal communication, July 14, 2022). In addition, the people are also confused with the functions and duties between NACSA and the agencies that handle issues related to cyber security such as MCMM, Malaysian Communications and Multimedia Commission (MCMC) and CSM, where in fact, NACSA is the coordinator and other agencies are the implementers. It should be known that NACSA focuses more on cyber security. It is different from information security managed by MCMM and MCMC (Md. Zain, S. N, personal communication, January 24, 2023).

In the event of an attack, there is a standard operating procedure (SOP) prepared for reference which indicating proactive action from NACSA. Constrain of some actions that make it slower. The cyber security issue most highlighted are due to many people and private sectors become the victims. Delay in taking action may be from the aspect of cyber security due to evidence issues. If the digital space can be identified, it can be handle in more good hands. The first action if a cyber security is detected, are the RMP which are suppose to make an immediate arrest to prevent the perpetrator from not admitting it and using someone else's identity. However, RMP is reluctant because they are unable to focus on cyber security issues as they have many other responsibilities (Md. Zain, S. N, personal communication, January 24, 2023). Nevertheless, the advantage is that NACSA is an agency under NSC and NSC is an agency under Prime Minister Department that reports directly to the Prime Minister. Compared to other agencies such as MCMM, MCMC and CSM, they need to report to the Minister and Director General first and then the Minister and Director General also need to consult with the Prime Minister. Therefore, NACSA is able to obtain results directly and it is in line with their position under NSC where NSC is the main coordinating agency for national security.

According to Shah Nuri, NACSA used to focus on critical knowledge infrastructure. Now NACSA develops it through an official website. MCSS is taking a long time to prepare, where previously NACSA had asked CSM and MARA Technological University (UITM) to prepare it but seems not succeed. Finally, Shah Nuri and other NACSA officer who prepared it managed to finished and succeeded. Now it is called Critical National Information Infrastructure (CNII) which involves small, medium and public enterprises in Malaysia. It is a massive implementation. NACSA tries to diversify its involvement. There are a total of 113 programs implemented including programs with the people. The Master Plan has five (5) target groups including the people, who have a specific approach and these programs are implemented in an integrated and coordinated approach for the National Awareness Program (Md. Zain, S. N, personal communication, January 24, 2023).

Shah Nuri stated that other countries such as Singapore, Australia and the United Kingdom also have good relations with NACSA. In the five (5) years of MCSS implementation, NACSA targets to produce 10 recognized products. Malaysia Digital Economy Corporation (MDEC) successfully implemented them with 100 cyber programs. In 2003, Shah Nuri represented Malaysia as a government expert group to the United Nation (UN), and proposed the establishment of a central agency, which reports directly to the Prime Minister. As a result, countries such as Singapore, United Kingdom and Australia have established it earlier than Malaysia. However, Malaysia is seen as having the best governance. Shah Nuri has tried to disclose this matter to the media but was not approved by the top management. It stems from NSC's work culture behind the scenes which is need to be changes (Md. Zain, S. N, personal communication, January 24, 2023).

After all, it can be seen that the cyber security crisis/threat has become our country and government priorities which also led to the establishment of NACSA for the purpose of coordinating and implementing it with other relevant agencies in order to combating these issues. The collaboration are with the MCMM, MCMC, CSM and Ministry of Communications and Digital where there are scholars who state that cooperation between these agencies are satisfactory through various approaches taken. NACSA acts as policy coordinator while these other agencies act as implementers. NACSA then coordinates each state to have an officer with knowledge in the field of cyber security where NASCA provides training, as a focal point at the state level. Previously, it was only managed by the central. It is showed that although NACSA is only at the central and there are no branches in the state, each state NSC have a special section to deal with cyber threats but needs to coordinate with NACSA. The increase in cyber security has also led NSC to update cyber-related Directives (NSC Directive No. 24 to NSC Directive No. 26) and NSP has also outlined measures to deal with cyber threats in all nine (9) core values. NACSA also created Cyber Security Awareness Master Plan (CSAMP) as the main reference in the cyber security awareness program implementation at the national level (Md Saad, R, personal communication, July 14, 2022).

It is also showed with the establishment of NACSA, eventhough the cyber security cases has shown an increase trend, cyber threat situation is still under control. The problem is due to the society not having awareness and giving space. National preparedness to deal with cyber threats cannot be faced alone and needs to be faced together. Cyber security issues now demand that NSC's role be publicized, where NSC which used to act behind the scenes has changed to become more prominent through increased communication for all parties to jointly look after the national security, but the level of secrecy must still be remain. The government feels that cyber security should be a priority for every country, especially in matters that underlie the economy and national security. The implemented approach by the government in dealing with cyber security issues takes a holistic approach. All government and private organization needs to consistently strengthen network security defenses. In addition, organizations need to build capacity and implement continuous training.

Besides the government, the people and private sector is in the view that there are many weaknesses that need to be improved in dealing with cyber threats such as in aspects of law enforcement, public awareness, systems, governance, technology, involvement of all parties, increased campaigns and public awareness of risks through education programs as well as coordination and vigilance of the agencies involved. Public and private also sees cyber security threats as a serious issue and impact the economy, defense, military and security of the domain. If cyber security is not dealt with collectively, it has the potential to create a big impact in various aspects and is capable of threatening the harmony and country security including threatening religious and racial aspects thus affecting the people unity. Weaknesses in law enforcement as well as the level of public awareness are factors on the increase in cyber security. Public-

private cooperation in the fight against cyber security can improve security aspects and smoothen the efforts. However, most of the perception showed that NSC is still managed to coordinate the cyber security crises/threats through NACSA. There is also no issue of sharing cyber information and only related to companies in other countries. Still there is difficulties in coordination between agencies related to competing in functions and roles. In addition, there are also suggestions that these agencies increase vigilance and coordination when there is still public confusion on the difference in NACSA roles and functions with other agencies.

The cyber security crisis/threat also seems to be politicized (there is political intervention/view) so that it gets the attention of the country and the public, when cyber security have increased at an alarming rate and cause a huge losses every year. Due to that, the government has tried to formulate and implement various initiatives to deal with it and reduce the risks that exist. One of them is through cooperation and engagement with the private sector. Many collaborations implemented with various joint initiatives, but there are still shortcomings and weaknesses in the coordination implemented.

Conclusion

Overall, this article breaks down the Malaysia NSC involvement in dealing with cyber security which are found as "proactive" through the "active" collaboration with other agencies but there are challenges in coordination that need to be addressed regarding the people ignorance and confusion in NACSA roles and functions. As for the coordination effectiveness between the central and state NSC in dealing with cyber security, there are no constraint and the researcher sees it as "effective". For the political interference analysis that affects the cyber security management effectiveness, it has an impact on the management decisions related to cyber security since there is a political membership related to cyber in the NSC Session. But still the political interference is minimal and there is no reason for interference.

The researchers suggested that the NSC through NACSA increase programs between agencies such as joint courses, sports/leisure activities, competitions and others, which are interspersed with activities explaining the functions and roles of each, to overcome problems related to confusion. In addition, NACSA also needs to increase programs with the people such as holding Customer Meet Days as well as campaigns and distributing brochures about NACSA roles and functions, also the people responsibilities, to overcome the problem of ignorance. For improvement, it is suggested that future studies analyze comparative studies about the effectiveness of Malaysian institutions with those abroad in dealing with cyber security issues so that it can be known how far Malaysia has achieved compared to other countries.

Acknowledgement: All the authors would like to thank the informants from NSC, MOHA and MINDEF who were willing to be interviewed in obtaining the study data.

Conflict of Interest: None of these authors that have any conflict of interest.

References

Bahaudin, N. H, & Haqimi, M. A. (2022, March 30). Ancaman keselamatan siber semakin serius. *My Metro*. https://www.hmetro.com.my/mutakhir/2022/03/826613/ancaman-keselamatan-siber-semakin-serius

Bansal, M. (2018). An Overview of Cyber Security in Malaysia. *Journal of Emerging Technologies and Innovative Research (JETIR), 5*(8). https://www.jetir.org/papers/JETIRFF06020.pdf

Bernama. (2022, August 5). *11,367 kes jenayah siber dari Januari hingga Julai tahun ini*. https://www.astroawani.com/berita-malaysia/11367-kes-jenayah-siber-dari-januari-hingga-julai-tahun-ini-polis-374682

Bernama. (2022, June 7). *Malaysia catat 57.8 juta serangan virus siber pada suku pertama*. https://www.astroawani.com/berita-malaysia/malaysia-catat-578-juta-serangan-virus-siber-pada-suku-pertama-fortinet-365120

BH Online. (2021, June 28). *Keselamatan siber lengkapi usaha memacu pertumbuhan ekonomi*. https://www.bharian.com.my/berita/nasional/2021/06/832966/keselamatan-siber-lengkapi-usaha-memacu-pertumbuhan-ekonomi-muhyiddin

BH Online. (2021, May 23). *Malaysia siap siaga hadapi ancaman siber*. https://www.bharian.com.my/berita/nasional/2021/05/819815/malaysia-siap-siaga-hadapi-ancaman-siber

Burton, J. (2013). Small states and cyber security: The case of New Zealand. *Political Science*, *65*(2), 216-238. https://doi.org/10.1177/0032318713508491

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber security risk management frameworks implementation in Malaysian Higher Education Institutions. *International Journal of Academic Research in Business and Social Sciences*, *12*(4), 1356–1371. DOI: 10.6007/IJARBSS/v12-i4/12300

E. Ite, U. (2004). Multinationals and corporate social responsibility in developing countries: a case study of Nigeria. *Corporate Social Responsibility and Environmental Management*, *11*(1), 1-11. https://doi.org/10.1002/csr.49

Fuad, N. S. M., Daud, M., & Yusof, A. R. M. (2022). Memahami Jenayah Siber Dan Keselamatan Siber Di Malaysia: Suatu Pemerhatian Terhadap Pandangan Sarjana Dan Intelektual: Understanding Cybercrime and Cybersecurity in Malaysia: An Observation from The Perspective of Scholars and Intellectuals. *Asian Journal of Environment, History and Heritage*, *6*(1), 11-26. https://spaj.ukm.my/ajehh/index.php/ajehh/article/view/184

Ganesin, A., Supayah, L., & Ibrahim, J. (2016). An overview of cyber security in Malaysia. *Kuwait Chapter of the Arabian Journal of Business and Management Review*, *6*(4), 12-20. https://platform.almanhal.com/Files/Articles/101388

Hamzah, A. (2004). Kaedah Kualitatif Dalam Penyelidikan Sosiobudaya: Qualitative Methods in Sociocultural Research. *Jurnal Pengajian Media Malaysia*, *6*(1), 1-10. https://sare.um.edu.my/index.php/JPMM/article/view/32755

Hasnan, H. A. (2019, April 3). Ancaman siber: NACSA bakal keluarkan Strategi Keselamatan Siber Negara. *Astro Awani*. https://www.astroawani.com/berita-malaysia/ancaman-siber-nacsa-bakal-keluarkan-strategi-keselamatan-siber-negara-203081

Ismail, I. S. (2022, September 22). MKN kesan peningkatan ancaman serangan siber. *BH Online*. https://www.bharian.com.my/berita/nasional/2022/09/1003536/mkn-kesan-peningkatan-ancaman-serangan-siber

Jasmi, K. A. (2012). Metodologi pengumpulan data dalam penyelidikan kualitatitif. *Kursus Penyelidikan Kualitatif Siri*, *1*(2012), 28-29. https://www.researchgate.net/profile/Kamarul-Azmi-Jasmi/publication/293097563_Metodologi_Pengumpulan_Data_dalam_Penyelidikan_Kualitatitif/links/5c0234e0a6fdcc1b8d4d2e10/Metodologi-Pengumpulan-Data-dalam-Penyelidikan-Kualitatitif.pdf

Krishnan, D. Bala. (2021, January 26). Brace for possible cyber-attack, govt agencies told. *New Straits Time*. https://www.nst.com.my/news/nation/2021/01/660733/brace-possible-cyber-attack-govt-agencies-told

Lai, R., & Rahman, S. S. (2012). Analytic of China Cyberattack. *The International Journal of Multimedia & Its Applications (IJMA)*, *4*(3), 37-56. https://doi.org/10.5121/ijma.2012.4304

Lehto, M., & Limnell, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139-148. https://doi.org/10.1080/19393555.2020.1813851

Liff, A. P. (2018). Japan's national security council: policy coordination and political power. *Japanese Studies*, *38*(2), 253-279. https://doi.org/10.1080/10371397.2018.1503926

Lilli, E. (2020). President Obama and US cyber security policy. *Journal of Cyber Policy*, *5*(2), 265-284. https://doi.org/10.1080/23738871.2020.1778759

Mat, B., Pero, S. D. M., Wahid, R., & Shuib, M. S. (2020). Cyber Security Threats to Malaysia: A Small State Security Discourse. *Sustaining Global Strategic Partnership in the Age of Uncertainties*, *5*(6), 31.https://www.researchgate.net/publication/349881373_Cyber_Security_Threats_to_Malaysia_A_Small_State_Security_Discourse

Matsubara, M. (2014). Countering cyber-espionage and sabotage: the next steps for Japanese–UK cyber-security co-operation. *The RUSI Journal*, *159*(1), 86-93. https://doi.org/10.1080/03071847.2014.895263

Medcalf, R. (2017). Imagining an Indian National Security Strategy: the sum of its parts. *Australian Journal*

of International Affairs, *71*(5), 516-528. https://doi.org/10.1080/10357718.2017.1342762

NSC Official Website. (2022, May 11). *Keselamatan Siber: Bahaya 'Espionage'*. https://www.NSC.gov.my/web/ms/2022/05/11/keselamatan-siber-bahaya-espionage/

Omar, S. Z., Kovalan, K., & Bolong, J. (2021). Effect of age on information security awareness level among young Internet users in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, *11*(19), 245-255. https://doi.org/10.6007/ijarbss/v11-i19/11733

Park, J., & Chung, E. (2021). Learning from past pandemic governance: Early response and Public-Private Partnerships in testing of COVID-19 in South Korea. *World Development*, *137*, 105198. https://doi.org/10.1016/j.worlddev.2020.105198

Rosli, F. A. (2020, May 26). Enam langkah 'lawan' jenayah siber. *Berita Harian*. https://www.bharian.com.my/berita/nasional/2020/05/692956/enam-langkah-lawan-jenayah-siber

Smith, F., & Ingram, G. (2017). Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*, *71*(6), 642-660. https://doi.org/10.1080/10357718.2017.1320972

Stevens, T., & O'Brien, K. (2019). Brexit and cyber security. *The RUSI Journal*, *164*(3), 22-30. https://doi.org/10.1080/03071847.2019.1643256

Suhaimi, F. (2020, November 4). RM1.8 bilion diperuntukkan, rangka Strategi Keselamatan Siber atasi jenayah siber. *Astro Awani*. https://www.astroawani.com/berita-malaysia/rm18-bilion-diperuntukkan-rangka-strategi-keselamatan-siber-atasi-jenayah-siber-saifuddin-266683

Zahri, Y., Ab Hamid, R. S., & Mustaffa, A. (2017). Cyber security situational awareness among students: a case study in Malaysia. *International Journal of Educational and Pedagogical Sciences*, *11*(7), 1704-1710. https://doi.org/10.5281/zenodo.1131053

Zaini, A. H. (2020). *Keberkesanan koordinasi agensi kerajaan dan isu pemerdagangan orang: Kajian empirik organisasi jenayah terancang dalam industri eksploitasi seksual* [Master's thesis, National University of Malaysia].

Zajko, M. (2015). Canada's cyber security and the changing threat landscape. *Critical Studies on Security*, *3*(2), 147-161. https://doi.org/10.1080/21624887.2015.1071165