Cyber Security Stagnation in Indonesia and the Philippines: A Comparative Case Study of their Strategies

July 2023

2718439K

21111014

85819125

Presented in partial fulfilment of the requirements for the Degree

of

International Master in Security, Intelligence and Strategic Studies

Word count: 21765

Supervisor: Marcin Kaczmarski

Date of Submission: 21/07/2023

Acknowledgments

I would like to thank Marcin Kazcmarski for his help during the writing of this thesis. I was often lost and the discussions we had helped me to get back on track.

Thank you to David Vauclair for helping me with choosing the topic and always being there when I needed help. You have been the most amazing teacher since 2018, and I am glad to be able to say that I can count you among my friends.

I would also like to thank Sopra Steria for giving me 30 days to finish that thesis, and especially to Constance Jourdan for being a great internship tutor. I have learnt a lot and it really helped me to write parts of this thesis. A special thanks to Constant Abraham, Nicolas Deat and Océane Crelerot for their support, their help to read my thesis and improve it. I would also like to thank the entire Cyber Threat Intelligence Team and Vulnerability Operation Center for their support.

Many thanks to Jeanne Esmangart de Bournonville (soon to become Jeanne Sambain) for her help in rereading all this thesis.

Special thanks to my thesis Zoom friends, who were always there for work sessions, especially Fiammetta Mondini for listening to all my problems and complaints and Gwenn Robert for her special ability to send me to work every time I needed to.

Many thanks also to my family, especially my mom, and close friends for their love and support and not being angry when receiving my daily word count, especially Elara Flament, Tifaine Vermet and Anne-Claire Pedo.

Table of content

List of Abbreviations

ANSSI: Agence nationale de la sécurité des systèmes d'information/ National Agency for Security of Information systems

APT: Advanced Persistent Threat

ASEAN: Association of Southeast Asian Nations

BIN: Badan Intelijen Negara/ Intelligence Service of Indonesia

BSSN: Indonesian National Cyber and Crypto Agency

CERT: Computer Emergency Response Team

CICC: Cybercrime Investigation and Coordinating Center

CSP CERT: Cyber Security Philippines CERT

DICT: Republic of The Philippines – Department of Information and Communications Technology

DND: Department of National Defense

DoS/DDoS: Denial of Service/ Distributed Denial of Service

DRA: Decisions and Risk Analysis

IDSIRTII/CC: Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center

IMSISS: International Master in Security Intelligence and Strategic Studies

KOMINFO: Ministry of Communication and Information Technology, Indonesia

NIST: National Institute of Standards and Technology

NCSI: National Cyber Security Index

OT: Operational technology

TNI: Tentara Nasional Indonesia/ Indonesian Army

SCADA: Supervisory Control and Data Acquisition

SBY: Susilo Bambang Yudhoyono

List of Tables and Figures

Abstract

This dissertation has the purpose to find out whether the cyber security strategy of Indonesia is a factor for its cyber stagnation. It is a comparative case study, in which I compare the reactions of Indonesia and the Philippines toward cyberattacks. These reactions being different, I chose to analyse the cyber security strategy of Indonesia focusing on the motivation of the country to have a cyber security strategy, the approaches used in this strategy, the structure of the strategy and its content. Each part will be analysed with the realist tradition, the constructivist tradition and the risk management theory. I will also take the Filipino strategy as a standpoint to demonstrate the various problems of the cyber security strategy of Indonesia. This dissertation will prove that the Indonesian cyber security strategy is largely responsible for the cyber stagnation of the country.

I. Introduction

On the 6th of July 2023, newspapers such as the Jakarta Post were publishing articles on the theft of 34.9 million passports by the hacker Bjorka.[1] The hacker had targeted the immigration office of Indonesia to conduct their attack. It is not the first time that this hacker is attacking the country and stealing data to sell them. In 2022, he stole 1.3 billion sim cards.[2] Indonesia is not the only country in Southeast Asia which is targeted a lot by cyber attackers, the Philippines have had its share of cyberattacks in the 21st century. It started with the famous worm I LOVE YOU, and nowadays the country is targeted every day by different types of threat actors such as state sponsored groups or ransomware groups.

To counter the growing number of attacks, Indonesia and the Philippines both published their cyber security strategies in 2014 and 2016. These documents aim to define the guidelines of the countries to improve their cyber security. In it, they define cyber security with the same criteria. Their respective strategies both acknowledge "the confidentiality, integrity and availability" of data. However, for the scope of action, Indonesia only mentions "information and all supporting facilities"[3] while the Philippines is more precise and indicates "computer systems, network systems, information systems, and other areas related to the protection of information assets".[4] If both countries have effective cyber strategies, the number of successful cyberattacks should decrease. However, the National Cyber Security Index (NCSI), which is evaluating how countries are ready to "prevent and manage" cyberattacks, has ranked Indonesia

[1] The Jakarta Post (2023)

[2] Llewellyn (2022)

[3] Indonesia Pedoman Pertahanan Siber. (2014)

[4] DICT (2016) National Cyber security Plan 2022.

84/195 and the Philippines 43/195.[5] The Philippines is therefore doing better in preventing attacks than Indonesia. The latter has had a tremendous number of attacks despite its cyber strategy. Therefore, I am observing a cyber stagnation. I am defining cyber stagnation as a state in which a country is not improving its cyber security which makes it vulnerable to cyberattacks. This can be explained by different factors, strategic, economic, technological, political, social. As it is the most relevant for my degree, I have chosen to explore the strategic factor.

This raises the following research question: How do the responses of the Indonesian and Philippine governments to multiple cyberattacks over time differ, and how might these distinctions in their cyber security strategies unveil the Indonesian cyber stagnation? This dissertation will focus on the strategy of Indonesia being a potential factor for its stagnation. It will be a comparison case study between the strategies of the Philippines and Indonesia as well as an analysis of the Indonesian cyber strategy.

This dissertation will start with a literature review on effective cyber security, Indonesian cyber security, and Filipino cyber security. In the second part, I will present the methodology. It will then move on to my theoretical framework, in which I will present the realist tradition, the constructivist one and the risk management theory. Afterwards, I will present the numbers of cyberattacks in Indonesia and in the Philippines, as well as the reactions of both countries to these cyberattacks, in order to compare them. This will show that Indonesia and the Philippines have different reactions. Therefore, in the next part, I will compare the Indonesian cyber security strategy and the Filipino one. Finally, I will study the Indonesian strategy's motivation, their approach, the structure of their strategy, and its content, to assess if it can explain the cyber stagnation of the country.

---

[5] NCSI: Ranking, (no date)

This dissertation will demonstrate that reactions of Indonesia and the Philippines toward cyberattacks are different. Therefore, I have studied the cyber strategy of Indonesia and discovered that it is partially responsible for the lack of effective cyber security in Indonesia.

II. Literature review

This part will present the literature on three topics relevant to this study. It will start by showing the views of authors on what makes a good cyber security. Then, the second part will present the literature on cyber security in Indonesia. Finally, the third part will expose articles on cyber security in the Philippines.

A. Effective Cyber Security: Risks, Framework and Education

a. Cyber Security Risks

Cyber security is defined by the French National Cyber Security Agency (ANSSI) as the "desired state of an information system that enables it to withstand events originating in cyberspace that could compromise the availability, integrity or confidentiality of the data stored, processed, or transmitted and the related services that these systems offer or make accessible. Cyber security uses information systems security techniques and is based on the fight against cybercrime and the implementation of a cyber defence." (Personal translation from French).

To create effective cyber security, it is important to identify the risks that are linked to cyber threats.[6] To do that, it is necessary to conduct a cyber risk analysis which will display the biggest risks and then the cyber strategy will be adapted to these risks.

According to Montibeller and Franco, choosing the right strategy is no easy task. It takes different types of resources such as economics, "human, and time".[7] They explain that gathering data to make the best choices is not difficult, however using those data is difficult as their number can quickly become

[6] Mylrea et al. (2017)

[7] Montibeller and Franco (2007)

overwhelming, and their content can be contradicting one another. Some of these data are also qualitative such as the reputation or the culture of the organisation. These data are very important to maintain but they cannot be quantified. The reason why these strategies are hard to write is because there is a lot of quantitative and qualitative data to be considered and preserved and multiple goals to achieve. To create a good strategy, the authors explain that there is a need to have a learning process inside the decision process. The Decision and Risk Analysis (DRA) Framework works in such a way that the strategy maker needs to "understand the decision situation", which means evaluating the situation in which the decision is taken. Then, he should "define and structure the fundamental objectives" to know what goals need to be attained. Following the establishment of the objective, the DRA recommends to "identify and create strategic options" and at the same time to choose which are more important by making compromises. As soon as this is done, "strategic options" must be assessed, "uncertainties" have to be identified, and the strength of these options should also be evaluated. The risks also need to be assessed and recommendations must be given to improve the strategy.[8]

Now to be more specific, I will introduce the literature on cyber risk. Paté-Cornell et al. present a cyber risk analysis framework which helps to identify the risks and assess them.[9] According to them, what is most important when a cyberattack occurs is the time between the moment it starts and the moment it is discovered. Indeed, an attack discovered earlier will do less damage than an attack which has already reached its goal.

To assess the risks organisations or governments can face, Paté-Cornell et al. have written several questions. They start by the identification of their

[8] Montibeller and Franco (2007)

[9] Paté-Cornell et al. (2018)

assets, their location, and their connections. Then, they ask about the "protection measures". Finally, they try to assess how bad it would be if a person external to the company were to access their network whether partially or totally. Then, after the assets' assessment, they try to identify what the risks are in terms of attackers. It could be cybercriminals, state sponsored threat actors, hacktivists, contractors or even insiders. The authors highlight questions such as "what do those people want?" and "what do they already have?" to enter the system. They also explain that organisations should be aware of their own vulnerabilities. The organisations should then assess the attack scenarios and the attack impacts.

To assess the attack scenario, the authors recommend the utilisation of the MITRE ATT&CK framework, which compiles all the tactics and techniques used by attackers. Here is a non-exhaustive list of them and what they mean. There are reconnaissance tactics, the initial access tactics, the persistence tactics, the privilege escalation tactics, the discovery tactics, the lateral movement tactics, the exfiltration tactics, and the impact tactics. The reconnaissance techniques are how an attacker chooses its victim. The initial access techniques are how an attack enters a system. The persistence techniques are the techniques used by an attack to stay into a system. The privilege escalation is how an attacker passes from a user to an administrator and in the end has more privileges which will make the attack easier. The lateralization techniques are the way an attacker moves into the system. The exfiltration are the techniques used to exfiltrate the data and the impact techniques are the effects that the attack will have.[10]

According to Paté-Cornell et al., an organisation needs to understand this framework and base their strategy on it with a protection for each tactic named above. It will help them to better evaluate the risks linked to these attacks and

[10] MITRE ATT&CK Framework (2023)

create a more effective strategy. The organisations should also assess the attack scenarios and the attack impacts. Finally, Paté-Cornell et al. discuss the attack impacts in terms of risks. They mention again the time as extremely important "to effectively control the damages". They explain the different impacts whether they are qualitative or quantitative. Those impacts, for example "disturbing the right course of a company", "damaging or destructing assets", are especially serious if the company cannot implement damage control. Often qualitative impacts lead to "business disruption" or even full interruption, a "loss of reputation", and loss of technology. These impacts generally lead to a quantitative impact and an economic loss. The authors then conduct three analyses and conclude that when it comes to cyber risk it is more interesting to look at the "relevant information" than basing a strategy on "past statistics". Indeed, their three cases show that quantifying risk and countermeasures help decrease the risk and help taking the right decision in a crisis.

They finally give four last recommendations: prioritise the most important asset in a crisis, base their analysis on past attacks and imagine future attacks to be sure to correctly analyse what is critical for the company or the organisation. Thirdly, think in advance what countermeasures you can put in place based on your data. Lastly, be sure that these countermeasures are affordable for your company or for your organisation.[11]

The quantification of the impacts is a point also emphasised by Montibeller and Franco, since they declare it as an outcome from the evaluated "strategic options".[12] The latter then needs to be evaluated and it is the topic of their article. It is a generalist approach to strategy making. They explore the Decision and Risk analysis which is useful to "assess […] strategic initiative".

[11] Paté-Cornell et al. (2018)

[12] Montibeller and Franco (2007)

This method works in such a way that "it decomposes a decision problem into a set of smaller problems". It allows the decision maker to analyse the smaller problem first and then "to integrate" the solutions found into the bigger solution to the bigger problem.

b. Cyber Security Frameworks

Many authors have tried to create frameworks for cyber security such as Fischer, Mylrea et al., Elkhannoubi and Belaissaoui, and Al Mehairi. In 2005, Fischer defined the main weaknesses in cyber security. To do so, he determines the main type of attacks that can damage either the government assets or the view of the public on cyber security. According to him, "service disruption", "theft of assets" and "capture and control" are the main threats to governments.[13] He then defines the main sources of risk which are components of the critical infrastructure, "software", "cyber security governance" and the "public knowledge or perception".[14] Concerning governance, Fischer explains that there is a need for balance between technology, operations and personnel and that an imbalance could produce vulnerabilities. The aspects of the governance are described in Fischer's paper. The latter explains that to write a good framework in terms of governance, there is a need to establish "goals", "strategies", "policies", "procedures", "personnel" and "extent of problems and perception". The goals should have three specific features. They should be "measurable and meaningful", and a basis to motivate people in respecting and improving them. As such, people should think of their obsolete material and update it. Finally, the goals should relate to the other parts of the framework that he had established earlier on.

[13] Fischer (2005)

[14] Ibid.

In 2005, Fischer wrote that people in the US were aware of the possibility of a cyberattack. However, there were many reasons that made people unprepared to face cyberattacks. For example, people thought that there is a need to have great knowledge concerning cyber security to protect themselves. There was a lack of education and training in cyber security. Companies and organisations refused to disclose the fact that they had been attacked so as not to destroy their reputation and lose the trust of customers. At the time, Fischer also identified that there were often laws that were dissuading companies from investing in cyber security. Fischer's findings include the fact that a single approach to cyber security would endanger the company or the organisation. He recommends that organisations and companies "adopt standards and certification", that they "promulgate best practices and guidelines", that they make risk analysis, and that they have their systems audited. He also advocates for a good and up to date training, and for security to be encompassed into the organisations' architecture.[15]

In 2022, Al Mehairi et al. made recommendations that are still relevant to the ones made by Fischer in 2005. They explained that the infrastructure of organisations should be flexible so that they can adapt to any cyber threats.[16] They also showed that cyber strategies should be tailored to the organisations that are implementing them.

According to Mylrea et al., the Building Cyber Security Framework is a risk-based approach which gathers the "identification, the protection, the detection, the response and the recovery" against threats. These five words are the basis of the National Institute of Standards and Technology (NIST) cyber security framework. These parts of the approach enable people to conduct "risk

[15] Fischer (2005)

[16] Al Mehairi et al. (2022)

framing" with the identification, "risk avoidance" with the protection, "risk avoidance mitigation, sharing and transferring" with the detection and the response and finally "risk mitigation" with the recovery.[17] Mylrea et al. explains that threat intelligence should be conducted to monitor the threat. Detection processes must be continuously launched to monitor the organisation's system. A methodology on how to respond in case of an incident happens on the system has to be written. The last part is the recovery plan, which will encompass the improvement to be made to be able to face a further attack, and good crisis communication to discuss with partners and third parties. On a more practical side, a chief information security officer should be able to "isolate the infected asset", have constituted regular backups of the data, and have gathered all the technical details necessary for the reintegration of the assets.

Based on the definition of the ANSSI, in 2015, Elkhannoubi and Belaissaoui also tried to establish a framework to determine what an effective national cyber security is.[18] They studied and compared the cyber security strategies of France, Belgium, the European Union, the United States of America and the United Kingdom, to find what was good about them and what needed to be improved to establish their framework. From their study, they proposed three main pillars that are necessary to create an effective cyber security: (1) the organisational pillar, (2) the legal pillar and (3) the technological pillar.

The first one is about "policy and formation". Elkhannoubi and Belaissaoui start defining policy by explaining that it is both an external and internal set of rules. It needs the involvement of "regional and local authorities" as well as "the public and private sector", the governmental and non-

[17] Mylrea et al. (2017)

[18] Elkhannoubi, H. and Belaissaoui, M. (2015)

governmental organisations, and "the associations". It will in the end, reach the eagerness of any citizen to respect and spread the good practices written in the policy. The authors then explain that the principal recommendations can be found in the ISO/IEC 27002:2013. This norm sets standards to have the best cyber security possible. It has recently been revised by the norm ISO/IEC 27002:2022. The first norm, for example, demanded management teams to be involved in security, and for an organisation to be created to manage the implementation of the policies into their application. It also demanded the continuous training of all employees. It required from the organisation to check that it was fulfilling all the legal and "contractual requirements" as well as respecting the "international security policies and standard". The new updated norm has changed the structure of the controls. It has added controls to make for IT services. Some of these controls concern "threat intelligence", "data masking", "secure coding", "monitoring" and "information deletion".

c. Cyber Security Standards

In 2018, Srinivas et al. have emphasised the necessity to have a minimum of standards in cyber security and cyber defence. They discuss the Security Policy Framework, a UK framework, which sets the "minimum security measures that the departments should implement".[19] The authors described the "cyber security requirements" which are necessary in computer networks. These requirements are the "confidentiality" of data and their "integrity", which mean that the data are both kept private and that no one has modified them. The next requirement is "authentication", which means a user's identity is verified with the correct credentials or with biometric credentials, or even with something received on another device, and ideally with a two factor or multiple factor authentication. Another requirement is the "availability" of systems: systems must remain available even in the case of an attack of denial

[19] Srinivas et al. (2018)

of service (DoS). The next requirement is “authorization”, which is guaranteeing that a permission is given to someone else before they do any legal action. “Physical theft of devices” is the next cyber requirement. Devices are often connected with others, therefore an attacker who has stolen a device could access important credentials and critical information. Then, “non-repudiation” means that a user who has performed an action cannot claim it was not them. Finally, “freshness” refers to the data having their date and time attached, which stops the attacker from using old information and for example using an old message in his attack.

Srinivas et al. also presents the different challenges an organisation might face with the standardisation of cyber security. The first one is “organisation challenges”, which are the challenges linked to the time and personnel needed to implement the standardisation. The second one is the question of which area needs to be standardised. Then the third one is “the lack of agility”, which refers to the lack of the capacity that an organisation has to implement these processes fast. The fourth challenge is the choice of which standard for which requirements. The fifth challenge is the economic one: some countries or organisations do not have the necessary means to follow expensive standards. The last one is the “lack of awareness”. Sometimes, organisations do not realise that they need a standardisation.[20] Srinivas et al. also gives more practical information of what to do to protect a system. To name a few, they list “antivirus software”, “intrusion detection and prevention systems”, “encryption” and regularly “operating system updates”. The last one is “lack of awareness” which is necessary for organisations to protect effectively as human mistakes are often how attackers gain initial access.

[20] Srinivas et al. (2018)

Here is a table which better explains how Srinivas et al. (2018) explain the cyber security requirements, the system protection, and the challenge in standardisation.

Srinivas et al. (2018)		
Cyber Security Requirements	**How to Protect a System**	**Challenges in Standardisation**
- Confidentiality - Integrity - Authentication - Availability - Authorization - Physical theft of devices - Non-repudiation - Freshness	- Antivirus software - Intrusion detection and prevention systems - Awareness - Encryption - Operating system update	- Organisation - Areas to standardise - Lack of agility - Which standard for which requirements - Economic challenge - Lack of awareness

Another way to implement effective cyber security is through education. Indeed, a lack of training can cause tremendous damage to an organisation or a company. Beyer and Brumel have identified that education and training concerning cyber security are often "perfunctory, episodic and inadequate". According to them, to be effective in terms of cyber security, the strategy should ally with human detection and technological detection.[21] These two authors consider that cyber security should be performed by IT professionals but also that everyone involved in a company, or an organization should have a basic training in cyber security, to avoid attacks and protect the organization better. To put in place this training, Beyer and Brumel explain that human resources, IT services and IO psychologist service should work together in order to create an effective training. Each of them can bring something to the table. Human resources are trained to organise training, IT services have the necessary knowledge and IO psychologists can assess it. The authors also recommend

[21] Beyer and Brumel (2015)

having feedback on the training so that it is possible to identify the gaps and improve the training, and in the end the cyber security of the organisation. Al Mehairi et al. make recommendations which confirm the sayings of Beyer and Brumel. In their article, they emphasise the need to have more training about cyber security.[22] They also highlight the fact that good cyber security goes hand in hand with cyber security awareness, which can be achieved with a good training. According to them, it is the role of the IT services to raise this awareness. Al Mehairi et al. also gives a role to the head of the organisations. They claim that to have the best awareness, the leaders should be involved in the security programs and endorse the security measures. They should also be the first to take cyber security training, in order to make the best decision when a cyber crisis happens.

B. Indonesian Cyber Security

a. State of the Art

Authors such as Farisya Setiadi in 2012 or Noor Halimah Anjani in 2021 are both stating Indonesia's development of its Information and Communication Technology domain has had great results on Indonesia's economy.[23] This tendency keeps growing as the internet economy should pass from USD 70 billion to USD 146 billion in 2025.[24] In order to improve the digital transformation of Indonesia, according to the Asia foundation, the Palapa Ring project has been set in place. This project has a goal to provide a fibre optic network all over Indonesia. According to Medina, it should be finished by 2045.

[22] Al Mehairi et al. (2022)

[23] Setiadi, F. (2012)

[24] The Asia Foundation (2022)

Both Farisya Setiadi and Noor Halimah Anjani are concerned about the growth of cyber threats and the need to have a strong cyber security.[25] Indonesia also published "Cyber Defence Guidelines" in 2014, which explains the different attacks Indonesia might be facing and at the same time provides an overview of the current situation.[26] They clearly state in the document that they have not yet implemented their cyber policy effectively, as they are still adapting the structure of their institutions to the cyber defence needs. The document also explains that their technology is currently being improved. Furthermore, the document shows how they are lacking human resources with the proper cyber skills to implement the policy, and that there is not yet enough training to have these people ready to work in the cyber domain.[27] It then sets some ground rules principles that need to be applied in the cyber defence matter, such as people who are in charge of cyber defence are supposed to have the competence to do it, and cyber defence should be integrated in the design stage of any policy or document. It also states that the Indonesian cyber system should be safe and resistant against cyberattacks to protect the country.

To improve their cyber security, according to Noor Halimah Anjani in 2021, Indonesia passed several bills and laws. The two most important the author is endorsing are the "Electronic Information and Transaction law", which was passed in 2008 and revised in 2016, and the "Ministry of Defense Regulation", which was passed in 2014. Anjani insists on their importance. The first one explains which cyber activities are prohibited and creates a legal framework of protection for electronic systems and transactions, safeguarding their contents from any unauthorised access or misuse, and the second one finally gives a definition of cyber security. It defines it in this way "National

[25] Anjani, N.H. (2021)

[26] Indonesia Pedoman Pertahanan Siber. (2014)

[27] Indonesia Pedoman Pertahanan Siber. (2014)

cyber security comprises all efforts to secure the information and the supporting infrastructure at the national level from cyberattacks"[28]

In its" defence white paper" of 2015, Indonesia is considering the cyber field as its "fifth domain used as a battlefield",[29] whereas in 2017, the UN released a report measuring the commitment to cyber security, indicating that Indonesian cyber security is weak.[30] Their report of 2020 shows a clear improvement in their ranking.[31] However, the National Cyber Security Index (NCSI) is ranking Indonesia 84/195.[32] According to Muhammad Syaroni Rofii, the perception of cyber threat in Indonesia is very low, as the government has not made an issue of it.[33] Moreover, according to Ulum, cyber culture in Indonesia has a negative impact on cyber security policies.[34]

b. The National Cyber and Encryption Agency (BSSN)

In 2018, an assessment of Indonesia, before and after the creation of the National Cyber and Encryption Agency (BSSN) was written by the two authors, Mulyadi and Rahayu. This state body was founded in 2017 and is in charge of cyber security and information security in Indonesia. These authors establish a picture of the cyber security in Indonesia, stating that there is a "lack of cooperation among government agencies, the lack of national strategies, governance, policies, regulations and infrastructure" and that cyber security has yet to be merged within these.[35] They make 6 assessments about the time that

---

[28] Anjani, N.H. (2021) p. 13.

[29] Indonesia Buku putih pertahanan Indonesia (2008)

[30] 'Global Cyber security Index 2017' (no date), p. 78.

[31] 'Global Cyber security Index 2020' (no date), p. 172.

[32] NCSI: Ranking (no date).

[33] Rofii, M.S. (2020)

[34] Ulum, M. (2018).

[35] Mulyadi and Rahayu, D. (2018)

precede BSSN. (1) Before the BSSN, Indonesia was barely starting the elaborating of their National Cyber Strategy on a legal standpoint. (2) Their national Computer emergency response team (CERT), Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Centre (IDSIRTII/CC), created in 1998, was only intervening on special cases and was in "the early phase of operations". (3) There was no "public-private partnership" that was concerned with cyber security only. (4) Indonesia did not have any common plan to improve that "public-private partnership". (5) There were few education strategies put in place on cyber security. Only 3 universities were teaching the subject. (6) The Indonesian law was very controlling on cyber security products, imposing on them a lot of tests. According to Mulyadi and Rahayu, the BSSN works as a coordinator between the different Indonesian such as the government, academics, the private sector, and the community.[36] They have the power to shape cyber security in Indonesia through "regulations, human resources, technology, and cooperation policies".

Some critics are still made against the BSSN by Saputra in 2019. The author claims that the mandate of the BSSN is not strong nor obligatory enough. There are still some important cyber matters that are legally appointed to other government agencies, which undermines the power of the BSSN.[37]

This information, combined with the lack of a body "responsible to supervise and coordinate cyber security organisation"[38] identified by Farisya Setiadi, raised many questions and gaps. Why are Setiadi and Anjani making the same report almost 10 years apart? If the Indonesian government is very committed to cyber security measures, why is it still not prepared to face it

[36] Mulyadi and Rahayu, D. (2018)

[37] Saputra, P.N. *et al.* (2019).

[38] Indonesia Pedoman Pertahanan Siber (2014)

according to the NCSI? The cyber guidelines have been written in 2014, therefore why are they not applied and what is blocking the government to do so?

C. Philippines Cyber Security

a. State of the Art

According to the National Cyber Security Index, the Philippines is ranked 43/195 which makes them better than Indonesia, however their ranking by the global cyber security index in 2020 is 61/182 which is lower than Indonesia.[39] [40] This means that they are not very committed to cyber security but that overall, they are more prepared to face an attack than Indonesia.

The Philippines have been partnering with the US, Japan, or Australia about cyber security. [41] However, Winger considers that the partnership with the US was harmed by the arrival of Trump and Duterte in power, since they do not have the same vision of a cyber security strategy.[42] A second issue, considered by Winger, is the difference of goals between the two strategies. The American strategy is focusing on "military cyber means" while the Philippines are more concentrated on cybercrimes and their "cyber infrastructure". This partnership was harmed by cyberattacks. Advanced persistent threats coming from China and Vietnam have launched disinformation campaigns in 2020 and 2017 according to Winger. Cyber security was in the background of the alliance in 2020, even though the cyber infrastructure of the Philippines was weak and targeted by China. Winger claims that this matter needs to be addressed in order to have a more efficient alliance and "support mutual security in the digital age".

---

[39] NCSI: Ranking (no date).

[40] 'Global Cyber security Index 2020' (2020)

[41] Manantan, M.B. (2019)

[42] Winger, G.H. (2022)

The reason behind the focus of the Philippines on cybercrimes is the worm "I LOVE YOU", which attacked the Philippines in 2000 and which highly harmed the Filipinos.[43] A worm is a type of attack that has the ability to duplicate itself into a network and spread itself into new computers, therefore affecting more victims.[44] The I LOVE YOU worm was spread with attachments in emails and was the beginning of phishing. It cost $10 million to the Philippines. It started spreading outside of the Philippines, which attracted the attention of the FBI, which discovered that the worm came from the Philippines. The cooperation between the American police and the Filipino police allowed them to find the creator of the worm. However, due to the lack of laws in the Philippines concerning cyber security, this malware conceptor was released and could not be charged in the US as well, even though the countries had an extradition treaty. As a matter of fact, the latter mentioned that only crimes that are qualified as crimes in both countries can make the culprit eligible for extradition. Winger explains that the rapidity of the two police working together is linked to the existence of the alliance between the two countries. The worm still left its mark in the Filipinos' minds, which explains their views on cyber security.

b. Cyber Security Strategies

In 2004 or 2005, the Philippines released their first cyber strategy, called the "National Cyber Security Plan".[45] This document had similarities with the American one, according to Winger. He speaks about "philosophical convergences" however he also mentions that the partnership between the two countries was not exposed in the document. This document was overshadowed by the global war on terrorism, and cyber security became a least important

[43] Winger, G.H. (2022)

[44] What Is a Computer Worm and How Does It Work? (no date)

[45] Philippines National Cyber Security Plan 2005 (2005)

matter for the Philippines. Cyber security became an important matter again in 2012, when Chinese hackers attacked the website of one university in the Philippines in order to claim that a territory disputed between the two countries was Chinese.

As a response, the government enacted the Cyber Crime Prevention Act in 2012, aimed at preventing cybercrimes.[46] In 2012, they also passed the Data Privacy Act, which pushes companies and government structures to adopt cyber security measures to protect the data of their customers or their population.[47] In 2017, said act was amended to include stronger penalties for individuals found guilty of cyberattacks. [48] Moreover, thanks to the cyber strategy, the Filipino government has passed several laws and regulations about cyber security. According to the Octopus Community, a tool set by the European Council to know all the laws and policies on cyber matter, they became a party to the Convention on Cyber Crime or "Budapest Convention" in 2018.

According to Manantan, the country has tried to improve its cyber security by "launching a National Cyber security Strategy Plan 2022" in 2016. The main focus of their strategy is cyber autonomy, according to the Asia Foundation. Also in 2016, in order to monitor, alert and remediate the cyberattacks, the Computer Emergency Response Team (CSP CERT) of the Philippines was created. It finally got its accreditation in 2018. It provides analysis of cyberattacks by determining the techniques and tactics to produce the most effective response to the attack.[49] The National Cyber Security Strategy aims "to provide strong cyber infrastructure and cyber security". The

[46] Republic Act No. 10175 (no date)

[47] The Asia Foundation (2022)

[48] Public Law No: 115-76 (no date)

[49] CSP-CERT® | Cyber security Philippines - Computer Emergency Response Team® (no date)

Philippines have therefore started to educate its population on cyber security matters, through a bachelor's degree. De Ramos argues that there is also a need for the Philippines to teach cyber security to children. [50] He explains that, with a correct education on cyber security, users will be more confident to try new personal strategies to improve their cyber security. If people receive the correct training, they will be more able to reduce the vulnerabilities in their security. De Ramos' study tested how people modified their behaviours when given different correct information. It showed that all people that obtained information related to their cyber security have modified and improved their security habits. The study revealed that for only one of the tests, financial constraints hindered the cyber improvements. People were unable to buy the protection as it was too expensive.

According to Hasib, "cyber security is a business strategy".[51] Based on this assessment De Ramos' point makes a lot of sense. He argues that there is a need for cyber security experts to teach other people how to perform a correct cyber security and be prepared.[52] In fact, according to Nadua et al., the Philippines has improved its cyber workforce, passing from 84 to 216 recognized cyber specialists in 2022.[53] The reason why there is so little cyber workforce is the lack of money to pay them. The authors are finding that the salaries are not competitive enough. The lack of training is also an issue for the workforce. When there is a diversification of threats and they are growing all over the country, a lack of new training makes the country unattractive for the workforce. Lastly, the authors explain that the third thing that makes the country unattractive is its lack of governmental positions about cyber security. As there

[50] De Ramos, N.M. and Esponilla Ii, F.D. (2022)

[51] Ibid.

[52] Ibid.

[53] Nadua, F. *et al.* (2023)

is no possibility to evolve in these careers, it is difficult to stay as a cyber worker in the Philippines. This is a point also made by De Ramos.

Even though there has been improvement in the way the Philippines handles their cyber security, the Asia Foundation in their report of March 2022 stated that cyber security is still an underestimated topic for Filipinos, and they speak about a "misconception" that led them to believe that there are no "serious threats" regarding cyber attackers.[54]

This literature shows us that the Philippines, even though they are more attacked than Indonesia, are overall more prepared to face cyberattacks. They have a partnership with the US and there are more improvements in their management of cyber security. It raises the following question: is the Filipino Cyber Security Strategy Plan enough to explain why they are more prepared to face an attack than Indonesia?

[54] The Asia Foundation (2022)

III. Methodology

A. Guiding Principles

a. Choice of Topic

I chose this topic because of my great interest in cyber security, geopolitics, and cyber threats. In 2022, I came to work as a cyber security analyst for a private company, which enhanced my interest in the topic. Concerning the choice of my case studies, I always knew I wanted to work on Indonesia as it is my main field of study for the past 9 years. My first degree was in English and Indonesian, and I have continuously tried to link my different degrees in this research topic. However, my research question has been difficult to find. When I was researching the topic of cyber security in Indonesia at the beginning, I was mostly ending up on research questions such as "Why is it bad?" or "What can be done to improve it?". These research questions are interesting, but they have been studied over and over again by multiple authors. I was having trouble shifting the viewpoint to do something different and unique. I looked at the multiple attacks over the years, such as the data theft of Bjorka who sold 1.3 billion sensitive data of the Indonesian people on the dark web in 2022[55], or the data breach of the Indonesian Covid-19 application which has 1.3 million users. Following the attack of Bjorka, a government official only declared: "if you can, don't attack. Every time data is leaked, the people lose out, because that's illegal access", and "If you want to embarrass the government, find other ways to do it." For the second attack, according to the penetration tester company Cyberland, neither the Indonesian Ministry of health nor the Indonesian CERT, IDSIRTII, have done anything after learning about the attacks.[56] The examples of these two attacks made me wonder why

[55] Llewellyn, A. (2022)

[56] Cyberlands (no date)

Indonesia is not really improving their cyber security, even if they have been attacked so many times over the past years.

b. Comparison Case Study

Having made that assessment about Indonesia, I had to find a way to answer that question. I decided to make a comparison case study as it seemed the most logical choice. It seemed logical because, to assess why a country is not improving its cyber security, it is easier to compare it with similar other countries and show if they have similar or different behaviour. To make my choice, I thought of various countries in the ASEAN such as Singapore or Malaysia, however they were not entering the criteria I had thought of. I wanted a country that had similar wealth capacities, that was in the same geographic area, and which was geographically similar to Indonesia. This is why I ended up choosing the Philippines.

Both Indonesia and the Philippines are Tiger Cubs. The latter are a group of states which are composed of Indonesia, the Philippines, Malaysia, Thailand, and Vietnam. These countries are called like this in reference to the Asia tiger economies which were Taiwan, Hong Kong, South Korea, and Singapore. The Tiger Cubs economies were called like this as they had known a rapid growth of their economies starting from 1980 to the end of 1990 after the implementation of policies which "opened their capital markets".[57]

Indonesia and the Philippines are also members of the ASEAN, both archipelagos and both located in Southeast Asia. Indonesia has more islands than the Philippines, but both still have to implement plans, policies, and strategies within diverse islands, and it is different from implementing them in a continental country. The Philippines also suffers a large range of cyberattacks

[57] Lin and Liang (2019)

and have recently implemented their national cyber security strategy, which makes them an even better country to compare with Indonesia.

c. Choice of Factors

Once I chose the country I wanted to compare Indonesia with, I had to determine the most relevant factors possible for this study. There were 5 factors that could be used to answer the question: the strategic factor, the political factor, the technological factor, the economic factor, and the cultural factor. The strategic factor refers to the national cyber strategy of the studied countries and is based on long-term conception of cyber security. Then, the political factor refers to what the government is currently doing to improve the laws in terms of cyber security. It differs from the strategic factor as it is a much more short-termed conception of politics in cyber security. The technological factor concentrates on the capacity or incapacity of Indonesia and the Philippines to have the technological means to pursue their goals regarding cyber security. The economic factor is about having or not having the financial capacity to afford these goals. Finally, the cultural factor would be a study on how Indonesians and Filipinos perceive their cyber security and how their views on the subject could stop or enhance the cyber security of their respective country.

Any of these factors could be a response to my research question, as they could all be stopping Indonesia from having good cyber security. At the beginning, based on my personal preferences, I had chosen the political and the cultural factors. The other factors were interesting too but as a student in International Relations, who lived in Indonesia for more than a year, it was the factors that interested me the most. It seemed to me that the technological and the economic factors were depending a lot on the political factor, so it made sense to me to start with the basis of the problem.

Concerning the political factor, I found some interesting statements from the Indonesian government and some laws that had been passed. I

investigated the reaction of the government to cyberattacks and checked the various laws passed by the government to improve their cyber security.

I found the cultural factor extremely interesting and at the beginning of this dissertation, I was willing to make a survey to study the perception of Indonesian people on cyber security and how it affected the cyber security of the country. I know how to speak Indonesian, which could have allowed me to write a survey in the local language Bahasa Indonesia. I had the possibility to send this survey to universities, thanks to my time as a student in Indonesia. I also had some contacts who could have been useful to send the poll to a large number of people. However, after some time and some reflection on this idea, I came to the conclusion that I did not have the necessary means to create and diffuse such a survey. This is the reason why I decided to operate a shift from the cultural factor to the strategic factor. A large-scale survey would have taken more time than I had to spread and to analyse especially if there were some open questions in it. While the strategic factor is easier to study, as Indonesia and the Philippines had both published their national cyber security strategy. Moreover, it made more sense to study the strategic factor as the International Master's in Security, Intelligence and Strategic Studies (IMSISS) degree I am following focuses on security and strategy.

The last shift that happened in the factors is that I decided to drop the political factor and only focus on the strategic factor. I made this choice because I felt like these two factors were going to overlap each other and that it would be difficult to analyse the strategy of the countries without speaking of the laws or decisions that the countries have passed or taken to pursue the goals set in their respective strategies.

d. Research Design

I will now present the research design for this dissertation. This research will be a qualitative analysis with a comparative case study.

I am comparing two countries, Indonesia, and the Philippines to assess their situations in the cyber space and their reactions to cyberattacks. If the comparison shows that their numbers and reactions were similar, I will try to understand if their strategies are the reason for both countries to have bad cyber security. If the comparison shows that their situations as well as their reactions are different, then my focus will be on Indonesia and their strategy. I will analyse the strategy of Indonesia, compare it with the Filipino one and determine if it is the reason for its cyber stagnation.

I will use different approaches to analyse the chosen strategy after the comparison. There will be the realist tradition, the constructivist one and the risk management theory. I will also use the literature review to assess the effectiveness of the chosen strategy as well as the other strategy from a comparative standpoint.

IV. Theoretical Framework

A. Approaches

This thesis can be framed in several different theories. This theoretical framework will display the following theories. It will start with the realist approach, the constructivist approach and finally, the risk management theory. In this part, I will try to explain what the approaches and theory are.

a. Realist Approach

Realist approach is a tradition that became popular in 1939.[58] Classical realism puts power and its pursuit as the root of all international politics. According to Forde, the realist tradition starts with Thucydides and its most known thinkers are Machiavelli, Hobbs, Spinoza, and Rousseau.[59] Morgenthau established three bases that explains this approach. Firstly, the main actors of realism are the states and the "decision makers". Secondly, he clearly made a distinction between national politics and international politics. Thirdly, "International Politics is the struggle for power and peace".[60]

Realism is based on the idea that people will put their "self-interest"[61] first over morality and will only want more power. Forde explains that it is that "self-interest" which allows rulers to either consider the "national interest" of a country as a moral precept or that moral precepts are just not part of international politics at all. As such he explains that it is the second explanation that makes the state believe that they have a right to "pursue their self-interest". Therefore, the state will constantly compete to have more capabilities in order to protect the national interest.

---

[58] Williams and McDonald (2018)

[59] Nardin and Mapel (1992)

[60] Vasquez (1998)

[61] Ibid.

Realist thinkers have three main beliefs. The first one is the "primacy of nation state". The second one is the rational behaviour of states and the last one is "the balance of power".[62] The approach is also based on "anarchy". The latter is the fact that in the current international system, states have no supranational body that would stop them in their sovereignty and their capacity to do whatever they want to.[63] Realists consider that it is the international environment states evolve which pushes them to fight for their "national interest". Moreover, it is that need to fight that pushes them to use potentially any means to achieve their goals.[64]

b. Constructivist Approach

The constructivist tradition is another approach that could help to understand this dissertation. This approach started to become popular in the 1980s.[65] Constructivism is a larger approach that has been applied to security studies. Constructivists argue that "security is a social construction". It means that security exists only because people construct it. Constructivists tend to talk about security in terms of practice[66] and focuses on the norms related to international security.[67] Farrell explains that norms are "beliefs" that concern the "social and natural world" which will in the end shape the "actors, their situations" and their capabilities to act.[68] These norms are "reproduced through social practice". They give a frame to what is possible to be done and what is not whether it is in terms of acceptability or effectiveness.

---

[62] Vasquez (1998)

[63] Williams and McDonald (2018)

[64] Nardin and Mapel (1992)

[65] Williams and McDonald (2018)

[66] Ibid.

[67] Ibid.

[68] Farrell (2002)

This approach differs from the realist one because it does not consider decision makers as rational but more as people within a "social structure". This social structure would be ruled by norms and these norms would either push people to act in a certain way or push people not to make certain actions because they would be inappropriate. Constructivists also enhance the idea of identity in international relations. They consider that it is the explanation behind decision makers "preferences", "interests" and actions within a certain realm. According to Ciolan, these identities and interests are created when actors are interacting with each other.[69]

If power was the most important thing for realists, constructivists consider that states decide to do things because they believe that they are the most appropriate thing to be done. They believe international norms is going to frame the actions of a state[70]. Farell gives an example in which states that newly got nuclear power will try to act the same way as states who already got it and therefore it will be possible to understand and predict their behaviour.

Concerning constructivism and cyber security, Ciolan starts by reminding the reader that actions made by decision makers are based on the perception they have of their environment which include the cyber space and the results of these perceptions.[71] She explains that "threats are social constructs" because they were created when actors started interacting and discussing them. She gives the examples of current decisions considering cyber security being based on "assumptions" and "scenario". On top of that, she explains that within agencies and expert communities, there are many actors that will have different opinions on how to deal with cyber security. Her conclusion

[69] Ciolan (2014)

[70] Ibid.

[71] Ibid.

is that national security as cyber security is established on perceptions of these threats whether they are real or not.

The second part of her analysis concerns the institutions and their actors. She explains that they are at the same time representative of the "norms, structures of interest and identities" and framed by the decision makers and how they apprehend their environment. She considers in 2014 that cyber security's norms were in construction and that there were yet to be international rules which will protect states and penalise cybercriminals. The cyber domain has entirely changed the perception of people of security. New norms need to be created as many concepts that were clear within the physical world became blurry such as the actors participating in a cyber war. These people could be trained militaries as well as civilians. Constructivists consider that new words within the lexical field of cyber security will help people set these new norms.

c. Risk Management Theory

The last theory in which this dissertation fits in is the risk management theory. I have written, in the literature review, how building an effective strategy is based on the perceptions of the risks in an environment.

So, as I explained in the literature review, risk management is a theory used to assess a situation and its risks. According to Jorion, its modern version became popular in "the mid-1990s".[72] It can be used to create a good strategy for organisations according to Montibeller and Franco.

According to Wildavsky and Dake, the risk is based on perception and "cultural biases" and "individual differences" have allowed researchers to predict the risk preferences of the studied subject.[73] Crockford argues that risk

[72] Jorion (2010)

[73] Wildavsky and Dake (1990)

management is a difficult notion as authors have difficulties defining what it is.[74] The author recalls the multiple definitions such as the definition of McCahill who explains that "risk management encompasses primarily those activities performed to prevent accidental loss". Other authors such as Bannister and Bawcutt are defining these "activities" in a more precise way. For them, it refers to "the identification, measurement and economic control". Crockford explains that the definition of "activities" is considering more the management part than the risk part as it first defines the issue, then looks at the possible decisions and chooses "the most appropriate" to the problem. The author explains that loss control is what truly matters for risk managers as it is what they are trying to achieve when they "identify", "measure" and "economically control" the risk.

As explained previously, Montibeller and Franco use the DRA framework which mixes the learning process and the decision process together. This article is using risk management to create a strategy. It starts by defining objectives through the analysis of the data whether they are qualitative or quantitative. The decision maker needs to consider all the potential uncertainties and find the best strategy. This strategy must be evaluated, and problems identified must be improved.[75] Once the assessment of the risks has been done, it leads to the possibility of using the Deming cycle.

The Deming cycle is a methodology which consists of four words: "Plan, Do, Check, Act". In his article, Matthews explains that this methodology is a tool which had been invented by Deming as well as other authors in order to create "Total Quality Management". This tool has interesting characteristics as it is "non-financial" and "a management approach for implementing

[74] Crockford (1982)

[75] Montibeller and Franco (2007)

improvement activities". It helps check the development of activities and adapt the initial plan to improve it.[76]

[76] Matthews (2011)

V. Comparison of their Numbers and Reactions

To answer my research question, I must present the numbers of attacks Indonesia and the Philippines are facing in recent years and compare them. Then I will introduce the short-term reactions of Indonesia and the Philippines to cyberattacks and compare them. Finally, I will present their strategies and compare them.

A. Key Numbers of Cyberattacks in Indonesia and the Philippines

I will start by presenting the number of cyberattacks in Indonesia and the Philippines and compare them.

a. Key Numbers of Cyberattacks in Indonesia

I will present the number of cyberattacks in the years 2021, 2022 and the beginning of 2023.

According to the "Indonesia's Cyber Intelligence and cyber security agency" in 2021, 1.4 billion cyberattacks hit Indonesian critical structures.[77] The company SocRadar, in their threat landscape of 2021, has established that 24 state sponsored groups, named or advanced persistent threat (APT), had targeted Indonesia. These APTs are sponsored by China, and Vietnam. Concerning the ransomware activity, groups such as "REvil, Conti, Avadon and Lockbit" targeted companies and government structures in the country. The ransomware groups conduct their attacks and then make double extortion, not only gaining money but harming the reputation of their victim by leaking their data to the public. This is done in order to push the victims to pay the ransom. All threat actors are targeting various sectors. The most targeted is the government, then education, digital media and entertainment, banking and

[77] The Asia Foundation (2022)

finance, e-commerce, healthcare and so on.[78] In 2021, SocRadar recorded 20,000 phishing attacks and 1 billion credentials were stolen to access Indonesian accounts. Threat actors use social media platforms, cloud, e-commerce, and payment apps to obtain initial access. The second most used vector of infection by threat actors is unpatched vulnerabilities of legitimate software. The third most used vector of infection in 2021 was the credential leaks, which means that attackers found valid credentials on the dark net and used them to access their victims' systems.

In 2022, there were 976,429,996 cyberattacks in Indonesia, according to the BSSN.[79] There is an improvement from one year to another. The company Kroll and its threat landscape of the Asia-Pacific region have assessed that there are three types of attacks that Indonesia is facing. Most of these attacks are malwares (35%), password attacks (23%) and phishing (15%).[80] Concerning the impacts of the cyber incidents Indonesia is facing, Kroll shows that the three biggest impacts are business disruption (62%), data loss (58%) and finally reputational damages (35%). Some state sponsored groups or advanced persistent threat (APT) were also observed in 2022 in Indonesia. One of them is named Earth Longzhi, a Chinese APT, was observed in March 2022 and targeted Indonesia.[81] Another one is Dark Pink, which targeted ASEAN and as such Indonesia.[82] Dark Pink has not yet been linked to any government but is mostly attacking government and military structures and its attacks are very

[78] '2021 Indonesia Threat Landscape Report' (2021).

[79] antaranews.com (no date)

[80] Kroll (2022)

[81] The Hacker News (2022)

[82] Tan, A. (2023)

sophisticated. By November 2022, Indonesia had already faced 700 million attacks and almost 40% of them were ransomwares.[83]

Since the beginning of 2023, according to SocRadar threat report, Indonesia has been targeted by at least "11 ransomwares" groups, "653 dark web threat", "2821 phishing attacks", and "1466 stealers", which are malwares specialised into credential theft and which allows the attacker to access the system with valid accounts. Lastly, 6 APTs were observed targeting Indonesia. These APT all came from China[84]. All these cyber attackers have targeted 64 different sectors in Indonesia. These numbers show that the cyber threats in Indonesia do not decrease. However, it is difficult to have the exact numbers as the year 2023 is not over yet.

b. Key Numbers of Cyberattacks in the Philippines

I will now present numbers on the cyberattacks that occurred in the Philippines in the year 2021, 2022, and the beginning of 2023.

MEC Network Corporation provided some numbers in terms of cyberattacks that hit the Philippines. In 2021, there were 623.3 million ransomware attacks that hit companies and governmental institutions. There were also 5.4 billion malwares attacks targeting the country in 2021.[85] Kaspersky Network Security also found "50 million web threat attempts" in 2021 and "380,000 new malicious files daily".[86]

In terms of business, the Philippines is the second most attacked country in the Asia Pacific region in 2022 according to Kroll while Indonesia was the

---

[83] Get to Know Ransomware Attacks (2022).

[84] SocRadar (2023)

[85] MEC Networks Corporation (2022)

[86] Philippines News Agency (2022)

fourth.[87] In 2022, 29% of attacks were malware attacks, 21% were phishing attacks and 13% were password attacks.[88] Impact wise, the three biggest were "business disruption" (60%), "data loss" (59%) and "theft of intellectual property" (43%). In 2022, Dark Pink, the APT previously mentioned, also attacked the country.

Since the beginning of 2023, according to SocRadar, there have been "75 dark web threats", "2 ransomware" groups observed, "203 phishing threats" and 1224 stealers. SocRadar has also observed 14 APTs which targeted the Philippines. These APTs were from China and Russia.

c. Comparison of their Cyberattacks

When comparing these numbers, I am clearly observing that Indonesia was more attacked in 2021 than the Philippines. Both countries are attacked by the same type of attacks, phishing attacks, ransomware and APTs. In 2022, the attacks continued but it seems that the Philippines was more targeted than Indonesia at the time. Then in 2023, it is back to Indonesia being more targeted than the Philippines.

Concerning the nature of the attacks, these numbers show that both countries are targeted by the same type of threats. However, there are more APTs targeting the Philippines than Indonesia and their attacks are generally more sophisticated and more dangerous. The fact that there are less APTs that have been detected in Indonesia does not mean that there are no on-going operations. It is possible that they have yet to be detected. In 2021, according to the company Mandiant, in the APAC region the median dwell time, time in between an APT starts its operation and is discovered, was 21 days.[89] In 2022,

[87] Kroll (2022)

[88] Kroll (2022)

[89] Mandiant (2022)

this number went up to 33 days.[90] These numbers show how attacks can be discovered a long time after it started and long enough for it to be very damaging for a country. Not knowing that Indonesia is under attack does not mean that it is not, but that they do not have the right means to detect these attacks and stop them.

There seems to be more ransomware attacks in Indonesia than in the Philippines. Ransomware attacks are less sophisticated attacks and Indonesia is more targeted by them than the Philippines.

Overall, if I take the most recent number of attacks detected by the company Kaspersky, I am observing that in June 2023 the biggest number of attacks was 60876 in the Philippines,[91] while in Indonesia it was 138641.[92] Again, there is a gap in the number of threats and I am showing here how, even though these two countries are touched by the same type of threats, Indonesia is way more touched than the other country, with a difference of 77763 attacks.

B. Reactions of Indonesia and the Philippines

Now that numbers have shown which country is the most attacked, I will present the reactions Indonesian and Filipino officials have when confronted to a cyberattack and compare them.

a. Reactions of Indonesia to Cyberattacks

As I have shown previously, Indonesia has had a lot of cyberattacks over the years. It is what pushed this country to implement a strategy in the first place. However, in this part, I would like to present the reactions of Indonesian officials in various cyberattacks. I would like to observe if there has been an

[90] Mandiant (2023)

[91] STATISTICS | Kaspersky Cyberthreat real-time map (2023)

[92] Ibid.

evolution between before the implementation of their strategies and after. In order to examine this, I will use two examples of attacks, one that took place before the implementation of their strategy and one after.

The first attack I have chosen occurred in 2010. It is the well-known Stuxnet attack. Stuxnet was a malware created by Israel and the US, which was meant to target Iran to sabotage their nuclear program.[93] The malware was created in 2005 but discovered five years later. It was exploiting Zero Days Vulnerabilities. These are a special type of vulnerability. It means that hackers have already exploited them before the software developers found them and have created something to patch them.[94] The malware was a worm, so it had the same reproduction capabilities as the I LOVE YOU one. It was designed to destroy the Iranian centrifuges. It was also designed so that legit machines do not show that there was a problem. The worm was discovered when it propagated itself outside of its prime target.[95]

As the worm duplicated itself, it ended up targeting Indonesia. Stuxnet targeted 34.000 computers in the country.[96] The newspaper Kompas explains that it is the 2nd most touched country by Stuxnet. This worm was dangerous for industrial companies as it was targeting the operational technologies (OT), and more precisely the "Supervisory Control and Data Acquisition" (SCADA).[97]

After extensive research in English and Indonesian, and after contacting Indonesian journalists about this topic, I have not found any evidence of a

---

[93] L. (2022)

[94] Zero-Day Vulnerability - Definition (no date)

[95] Ibid.

[96] Wahono (2010)

[97] Ibid.

government public statement or declaration about Stuxnet. Articles were written about this topic, but no government communication has been made.

I will now talk about the second attack I have found which occurred after the strategy was published by the Indonesian government. At the beginning of September, the threat intelligence branch of the company Recorded Future, Insikt had declared that ten Indonesian government agencies including their intelligence body Badan Intelijen Agency (BIN) had been attacked.[98] They declared to have found the breach in March, and that they told the Indonesian government twice in July and in June.[99] The attack was attributed to Mustang Panda, a Chinese APT. This threat actor conducts cyber espionage for political and economic motivations. It used PlugX malware, a remote access trojan, which had inserted itself in the government's networks. PlugX is used to steal data and stay on the system of its victim.[100] Remote access trojan is a category of malware which is used to gain "full administrator privileges and remote control of a target computer".[101]

In this case, the Indonesian government did react to the attack. Their ministry of communications (Kominfo) issued a statement about the attack, saying the BSSN was in charge.[102] The BIN, the BSSN and their respective spoke persons also made a statement, claiming that their experts had not found any trace of Mustang Panda in the IT systems of the BIN. Another security expert was more worried that the BSSN should be absolutely positive about the system's safety.[103] Advanced persistent threats such as Mustang Panda have a

---

[98] Cimpanu (2021)

[99] Hastanto (2021)

[100] Nair (2021)

[101] Yasar (2022)

[102] Agustini (2021)

[103] Footnote 95

lot of capabilities, as they are financially supported by states. In my opinion, it is possible that they have the capacity to hide within legitimate applications in the network.

I am observing here an evolution in how Indonesia is treating cyber security incidents. They used to have no reaction toward cyberattacks. This does not mean that the Stuxnet issue had not been discussed internally, but no actions had been taken. In 2021, Indonesian officials did react to the threat of a cyberattack. Even if some of them take the threat lightly, others are asking the BSSN and the government to take it seriously and take actions.

b. Reaction of the Philippines to Cyberattacks

The Philippines have also had their share of cyberattacks. As I did before, I will now present reactions to two different attacks, which respectively took place before their first strategy, in 2004, and after its implementation in 2016.

The most known attack is the I LOVE YOU attack. I have already explained the circumstances of the attack in the literature review. Therefore, I will only address the reactions of the government in the Philippines. The year the I LOVE YOU attack happened, the government of the Philippines could not charge the attacker, as they did not have any law about it. They worked with the USA to find the culprit. Their first reaction was to pass a law to frame E-commerce practices in which they could "punish computer crimes".[104] This law was not retroactive and therefore the attacker was never punished. The next year, in 2001, the Philippines created "forensic laboratories" to study cybercrimes.[105] In 2004, they published their first cyber strategy.

---

[104] Philippine President Signs Law to Punish Computer Crimes (2000)

[105] Sy (2015)

This shows how the Filipino government was reactive right after their first big attack. Afterward, they have consistently had congresses about cyber security and passed laws such as the "Computer Abuse Act" between 2004 and 2007.[106] Then, they criminalised diverse types of attacks, such as phishing in 2007 and spyware tools in 2008. Also in 2008, they criminalised typo squatting. In 2009, they started to discuss the "Cybercrime Prevention Act", which was finally considered constitutional in 2014.[107] It criminalised seven cybercrimes and created a "Cybercrime Investigation and Coordinating Center". The Philippines have consistently tried to improve their laws, so as not to be in a situation in which they could not penalise an attacker. In 2016, they published their second cyber strategy, so the next attack I chose to present will show the reactions of the Filipino government about an attack occurring past their second cyber strategy implementation.

The second attack I would like to speak about occurred in 2020. It was attributed to LuminousMoth, a Chinese APT. The group seems linked to MustangPanda.[108] They have targeted more than 1400 victims in the Philippines, using spear phishing emails and compromising USB to get initial access and deploy their payloads.[109] They picked out people who were working in governmental institutions. This campaign was made to steal data and cookies from their Filipino victims.

The Filipino government reacted through their CERT to the attack. The organisation firstly explained how the attack was conducted. Secondly, they gave recommendations to improve their cyber security. These recommendations

---

[106] Sy (2015).

[107] Ibid.

[108] Lechtik (2021)

[109] Ibid.

are very broad. They include patching the known vulnerabilities, protecting the data, checking if the devices are secured and giving cyber security courses to employees so that they can avoid human mistakes.[110] These recommendations fit what Srinivas et al. have written in their papers.[111]

c. Comparison of these Reactions

Comparing the information I gathered, we observe that the reactions of the two governments were very different.

During the first described attacks, Indonesia and Indonesian officials did not communicate on the topic. Even though they were the second most attacked country and Stuxnet was hurting the Indonesian industry, the government did not make any statement. On the contrary in the Philippines, the government reacted strongly when the attack happened and created laws and strategies to counter any future attacks.

Now for the second attack I described in this part, there is also a difference in how both countries reacted. This time Indonesia did take action. However, the company Kaspersky stated that they told the country twice before they publicly denied the attack. It is an interesting reaction in my opinion: it seems like the Indonesian government did not want everyone to know that they had been attacked by MustangPanda. However, denying the attack means that a company that has the expertise in tracking threat actors since 1997 would have mistaken the presence of MustangPanda. In my opinion, it is much more realistic that MustangPanda had the capabilities to hide themselves in the Indonesian network and it would be the reason why Indonesian experts did not find them. Cyber specialists also reacted to the attack. However, it is strange

[110] CERT-PH (no date)

[111] Srinivas et al. (2018)

that some did not take it seriously. It shows how Indonesia is still not taking cyber security seriously compared to the Philippines.

If you take the Filipino reaction, Kaspersky was also the company who uncovered the attack. The Philippines reacted and provided the adapted solutions to keep their systems safe. Their reaction was much more proportional to the attack than Indonesia.

C. Findings

In the introduction, I explained that this dissertation could go both ways, depending on the comparison of the numbers, reactions and strategies of Indonesia and the Philippines. It appears that the Philippines and Indonesia do not have the same situation and are not reacting in the same way to cyberattacks.

In terms of numbers, the comparison showed there is a difference in the number of attacks. Overall, Indonesia is much more attacked than the Philippines. The Philippines had more sophisticated attacks for the beginning of 2023 than Indonesia. However, just looking at the numbers, it is Indonesia that is the most attacked. An explanation for the difference in the number of attacks is that the Philippines have better cyber security than Indonesia and therefore are more prepared than Indonesia to face ransomware threats. It seems like Indonesia is still very much under attack even after having launched their cyber strategy.

In terms of reactions to this high number of attacks, there has been an evolution in how both countries reacted. The Philippines did take action when the first big malware hit them, but they did not have the laws to properly do something about it at the time. They now have changed their legislation to be able to fight against cyberattacks better. The Indonesian government used to not react at all to attacks, it changed over the years, and they now respond when threatened, however their reactions are still not proportioned to the level of

threat cyberattacks represent. The topic of cyber security is much more important in the Philippines than in Indonesia, and they used the experience they gained from their first cyberattack way better.

This comparison shows that the two countries are reacting differently to cyberattacks and therefore this dissertation will now try to understand if the strategy of Indonesia is responsible for its stagnation in terms of cyber security.

VI. Analysis

Now that I have assessed that Indonesia and the Philippines are not reacting the same way, I will present the strategy of Indonesia and the Philippines. I will then compare them and analyse in a second part if the Indonesian strategy is the reason for their cyber stagnation. The analysis will be on the motivation to create the strategy, the approach used, the strategy making and the content of it. Finally in a third part, I will discuss if there are other factors that can be taken into consideration for the stagnation.

A. Cyber Strategies of Indonesia and the Philippines

I will first present the cyber strategies of Indonesia and the Philippines, and I will compare them. This will help me to analyse the cyber strategy of Indonesia in the next chapter and understand if their strategy is the reason behind their stagnation regarding cyber security.

a. Strategy of Indonesia

The theory's name is Cyber Defence Guidelines written by the Ministry of Defence in 2014. The first chapter of the Indonesian cyber strategy defines the purpose of the document and which infrastructures are concerned by these guidelines. Their objective is to strengthen the national defence and be the main reference set to develop and implement cyber defence within the Ministry of Defence and the Tentara Nasional Indonesia, which is the Indonesian National Armed Forces (TNI). It defines its critical infrastructure as "defence and security, energy transportation, financial system, and various other public services".[112] These critical infrastructures are the ones that the country cannot spend more than a certain number of days without.

The second chapter presents the different types of threats that exist in cyberspace. Afterwards, it establishes the current situation of the Indonesian

[112] Indonesia Pedoman Pertahanan Siber (2014)

policies, institutions, technologies and human resources and its current needs, in order to improve it.

The cyber guidelines third chapter presents the main objectives to reach in terms of cyber defence. The document lists six objectives which are (1) comprehend the current situation, (2) make people from the defence minister and the army more conscious and educated on how to handle a cyberattack in the defence sector, to protect critical infrastructure, (3) integrate the different parties (ministers and army) in the cyber defence, (4) develop resources of cyber defence to integrate them in the national defence system (5) have different types of strategies to deter, take actions or recover, and (6) have a referential for infrastructures to better prepare, build up, and achieve cyber defence.

The document provides tasks that the Indonesian Ministry of Defence and the army must fulfil. The roles and functions of the Ministry of Defence and the TNI are also detailed and include maintaining the security of the Indonesian institutions and building systems and protocols that are resilient in case of a cyberattack.[113]

The fourth chapter of this document details the implementation of cyber security with a new framework, which include "policies, institutions, technology, and human resources".

It starts by presenting all the policies that are relevant and needed to be followed. The document states that each policy of the government must follow the guidelines and shows which policies are relevant to it. Those guidelines do not only explain how the cyber security policies of Indonesia are supposed to be implemented but also how the future policies, control objectives, protocols and approaches need to be chosen, in accordance with the previous policies and

[113] Indonesia Pedoman Pertahanan Siber (2014)

legislation, to ensure the best cyber security possible and fix the current issues. The guidelines require a risk management approach within organisations, to assess which risk is acceptable in order to improve cyber security. It suggests that the Ministry of Defence and the TNI should have a procedure in place to monitor, assess and control their systems, to quickly identify any errors, rectify them, prevent future security breaches, and evaluate the effectiveness of their measures to address the issue.

The second section is about standards. It lists ten different standards and norms that should be respected by governmental bodies to ensure a good cyber security. These are Indonesian, American, and European standards, such as the ISO ones or the NIST recommendations. ISO are norms on diverse topics such as security, quality management, energy management and so on.[114] NIST has created a framework which is used in order to help organisations to decrease the risk of cyberattacks.[115] This framework encompasses these stages so that organisations can “identify” the risk, “protect” themselves, “detect” the cyberattacks, "respond," and "recover" from them.[116]

The next section deals with cyber security implementation within institutions. It clearly states that those bodies should be tailored to fit the cyber security guidelines and not the opposite. However, on the next line it also explains that the institution can be developed separately. In this section, they focus a lot on the authority in charge of cyber security.

[114] Iso (no date)

[115] NIST (no date)

[116] Ibid.

It then moves to the technology section. In it, they recommend the use of data centres and technology which is supposed to be used especially for defence purposes.

The guidelines also cover the human resources training, which must be completed to be cybersecure. They make recommendations at the human resources level and claim that they are the most important asset. As such, they are considering human resources as needed to be competent. This is for them the biggest challenge: since cyberspace is a sector that evolves quickly, competences must be updated regularly. They create an entire process of recruitment in the strategy. Then, they present their awareness training program, which is used to improve knowledge on cyber security, on how to deal with incidents and improve technical knowledge of the employees.

They also present the stages of cyber defence implementation, with its prevention stages, its monitoring stages, its analysis stage, its defence stage, its counterattack stage, and its information security stage. The last part of the guidelines presents the stages of the cyber defence activities such as preparation, a timetable of what must be done and in which order and the different outputs that are expected and if these goals are reached, which steps can be implemented after and their outputs.[117]

b. Strategy of the Philippines

The strategy's name is National Cyber security Plan 2022, written in 2016 by the "Department of Information and Communications Technology" (DICT) of the Philippines. The main objectives of this plan are to focus on safeguarding the uninterrupted functioning of the critical infrastructure as well as the public and military networks of the nation. This involves the implementation of measures that promote cyber resiliency, ensuring the ability

[117] Indonesia Pedoman Pertahanan Siber, 2014

to respond effectively to threats both before, during, and after an attack. The plan aims to achieve this by establishing effective coordination between the relevant law enforcement agencies, and by promoting awareness and education among the public to create a society that is well-informed about cyber security issues.[118] The strategy is bound for all governmental entities of the Philippines as well as the "private sector, the civil society, the academe including the private individuals".[119]

The strategy starts by presenting the sources of the threat actors that are attacking the Philippines. It continues with the presentation and explanation of the framework put in place by the Filipino government to counter cyberattacks. The framework is represented by a three layers pyramid[120] presenting which body is in charge of which action, in which scope and to which aim. It also highlights the "interrelations" between all the leading bodies. It takes into consideration law making and enforcement, cyber threat intelligence, and cyber defence. In the document, it is twice mentioned that the country is at an "infancy stage" and that the strategy is made to make them reach cyber maturity. This shows the consciousness of the country of their own capacities. The document also explains how the government should stop only reacting to cyber incidents to already be proactive about them in their policies, by creating policies that are respecting the strategy and the framework. It also points out the fact that those policies should be adaptable so that they fit the social changes.

The strategy outlines a series of fundamental principles that the framework must uphold, including respect for the law, the principles of autonomy and self-governance, international cooperation, and a balance

[118] DICT National Cyber security Plan 2022 (2016)

[119] Ibid.

[120] Annex 1

between the free flow of information and individuals' privacy rights. Additionally, the framework should utilise a risk-based management approach.[121] It also presents the different actors in charge of cyber security such as the DICT, the CICC, the law enforcement and prosecution agencies and the Military.

The document also emphasises the role of people in the fight to create a cyber secure society: the strategy mentions the collaboration that they are putting in place in order to fight cybercrimes, whether it is at a national level or public and private collaboration. It is also presenting a "cyber security maturity model" which has five stages: Reactive and Manual; Tool-Based; Integrated Picture; Dynamic Defence; and Resilient Enterprise. The document considers that the Philippines is currently at the Reactive and Manual state which is explained as a stage in which the state is trying to fix the problems rather than finding the roots of those. They also state their willingness to arrive at the last stage, which is about developing a predictive and mission-focused approach to mitigate the impact of cyberattacks. This involves isolating and containing any damage caused by such attacks, securing supply chains, and protecting key critical infrastructure to ensure uninterrupted operations. By doing so, they would aim to minimise the disruption caused by cyberattacks and maintain the continuity of essential services.

The strategy shows how the Philippines are self-aware about their own situation and presents a series of actions that should be taken to improve the current situation of the country. They have grouped them by themes which are as follows: "Protection of Government Networks", "Protection for Supply Chain", "Protection of Individuals". Each theme has many points and programs that need to be fulfilled or created in order to achieve the Filipino goal.

---

[121] DICT National Cyber security Plan 2022 (2016)

Finally, the document ends by proposing two approaches to tackle the issue. Firstly, the active approach will be used to identify the resources required to support an organisation's critical functions. This will enable the government to provide the necessary resources and make well-informed decisions to ensure the smooth functioning of the organisation's most important activities. The active approach will also be used through "protective technology, awareness and training" to make sure that the strategy is enforced. Then the active approach will be utilised to detect the cyberattacks and respond to them appropriately. Finally, it will be employed in the recovery process to be more resilient toward the diverse attacks.

Secondly, the proactive approach will be used to create a "defence mechanism" to develop layers that will decrease the vulnerability of the country. The proactive method will then be used to deter attackers. The Filipino government wants to have multiple plans to be able to choose the most appropriate one depending on the type of attack. Lastly, the proactive approach will be used to develop the field of cyber security based on the needs of the Filipinos.[122]

c. Comparison of the Two Strategies

In this part, I will compare the two strategies. I will start by presenting a comparison that has been made by the Asia Foundation and then I will add elements to their comparison in terms of structure and content.

The Asia Foundation has very clearly assessed the elements that were present in the two cyber security strategies. They have made the comparison basing themselves on the two following categories: type of stakeholders and focus of strategy.

[122] DICT National Cyber security Plan 2022 (2016)

In terms of stakeholders, while the Philippines have various stakeholders such as businesses, citizens, critical infrastructure and government, Indonesia only has critical infrastructure as a stakeholder. The focus of the strategies is also different. While the Philippines have various focus such as the "CERT," "the critical infrastructure protection", the "cyber security awareness and education", "the knowledge of cyber security in the workforce", the "cyber threat/ cyberattack response", "the International and regional cooperation", "the policy legislation, and rule of law", "the privacy, freedom and human right protection", the "risk management", the "strong cyber security, defences and defend systems", Indonesia is focusing on "critical infrastructure protection", "national security" and "research, development and innovation". This makes sense with their respective strategies.

I will hereafter make the structural and content comparison of the two strategies.

In terms of structure, the Indonesian strategy is longer than the Filipino one. What is obvious when looking at the content is that Indonesia's two first chapters are only in one chapter in the Filipino strategy. Their third chapter corresponds to the second chapter of the Philippines in terms of content, with both speaking about the principles and the roles and responsibilities. The Indonesian fourth chapter and the Filipino third chapter are talking about the implementation of the strategy. The Filipino strategy is starting this chapter by presenting the key program areas while the Indonesian one is presenting its framework of defence implementation with the policies. The Philippines is then dividing the next two parts into active and proactive approaches. One of them is about detecting the threats and fighting them, and the second part is about deterring the threat actors so that there are less incidents. Indonesia is mixing both approaches in one chapter and is then going back to how to implement it with four different stages.

Table 2: Structural Comparison of the Chapters

Indonesia	**The Philippines**
	Introduction
Introduction (1)	Scope (1)
Cyber Defence Emergency (2)	
Cyber Defence Key Points (3)	The National Strategic Context (2)
Cyber Defence Implementation (4)	Key Strategic Initiative (3)
Closing (5)	Conclusion

In terms of content, the first difference I have observed is in the goal of both strategies. The target of the Indonesian strategy is only the minister of Defence, while the target of the Filipino one is way larger since they target the public and the military sectors.

Another difference I have observed is in the goal of both strategies. The target audience of the Indonesian strategy is only the Ministry of Defence while the target of the Filipino one is larger. They target the public and the military sectors.

Both strategies are then explaining who are the threat actors that are targeting their countries. Both strategies are discussing the definitions, the roles of their institutions and their actors, however, the space allocated for it in the Indonesian strategy is way longer than the one of the Philippines. The Philippines then moves on to their framework of analysis, which is establishing

who oversees which part. Indonesia does a similar part in its strategy. However, the Filipino strategy has many different bodies which oversee cyber matters. For instance, the DICT is in charge of the CERT; the Cybercrime Investigation and Coordinating Centre (CICC) of the cooperation between agencies; the Department of National Defence (DND) of "National Cyber Defence" and so on[123]. Indonesia is only giving roles and tasks to the army and the Ministry of Defence.

One important difference between the two strategies I have observed is that the Filipino one is assessing its current situation and the current level of cyber security in the country, while Indonesia is not. The Philippines is stating that they are only at the beginning of cyber security implementation twice. In comparison, Indonesia starts by the aims and objectives without at any time explaining what the current situation in Indonesia is nor giving an assessment of it.

The Filipino strategy is also giving principles to be respected by the entities of the framework, such as autonomy or international cooperation, which is not given in the Indonesian strategy.

Both strategies are explaining how policies should be adaptable to the cyber strategy. However, the Filipino one is adding that it should also be adaptable to "social changes". Indeed, the Filipino document is talking a lot about having a cyber secure society, while Indonesia is focusing on the military aspect only.

Both strategies are putting in place a risk management-based strategy. Indonesia is talking about the standards that the country must respect, and the Philippines is mentioning standards but is not making an entire part about it. A

[123] Annex 1

common ground between the two countries is that both want their institutions to be tailored to their strategies, but Indonesia is also saying that they can be developed separately. The Philippines is also making a lot of recommendations on the creation of university degrees in cyber security.

The Philippines is also proposing collaboration with other countries as well as “public-private partnership” to improve their cyber security. Indonesia is barely speaking of collaborating with another country for their cyber defence.

Another thing to compare is the approaches given. The Philippines is giving two different approaches: active and proactive. Indonesia is not really giving approaches strictly talking. They avoided using the NIST framework as their big categories. However, it seems like their way to implement things corresponds to the active approach of the Philippines, as well as a little like the proactive stage. Their prevention stage corresponds to two different parts: one is previously discussed by the Filipino strategy, which includes creating degrees in cyber security, and one is in their active approach, which is “protect”. Indonesia’s part on monitoring the attacks corresponds to the identification part of the Philippines. The Indonesian analysis stage corresponds to the detection stage of the Philippines. The Indonesian defence stage corresponds to the Filipino response stage. The Indonesian information security improvement stage corresponds to the recovery attack stage of the Philippines. The last stage, which is counterattack, corresponds a little to the deter part of the proactive approach of the Philippines, however that part is not developed at all.

Another part to compare is what they want to implement. The two countries are presenting concrete actions to implement their strategies. On one hand, Indonesia is mixing technological measures with policies creation measures, human resources measures and legal measures, and this in each of its five sections (“prevention”, “monitoring”, “analysis”, “defence”

"counterattack" and "improvement")[124]. For each solution, the Indonesian strategy is making an estimation of the potential outputs but without correlating one another. On the other hand, the Philippines is having an entire part on key strategic initiatives, which are the measures they want to implement. The strategy is sorted in different areas, "protection of critical infrastructure", "protection of government networks", "protect supply chains" and "protection of individuals"[125]. Each of these big areas is giving very concrete measures, to be taken by the government, and the order in which said measures should be taken. Their approach is more high-level, which means that they are not proposing technical measures but suggesting to create the entity or the program which will deal with the technological part. Their areas rarely mix every type of measure in the way Indonesia does. Their solutions are more elaborated as well, each of them has at least one paragraph allocated to it while Indonesia is only allocating a sentence or two to their solutions. This makes the Filipino strategy clearer.

At the end of the Indonesian strategy, they are giving an order for the steps that need to be implemented. It is anchoring the first recommendations within time. This does not exist in the Filipino strategy, as they are already doing it within the recommendations.

Comparing the two strategies, I realised that the Philippines seems far more prepared than Indonesia. On one hand, the strategy of the Philippines is well structured. They frankly use the NIST framework as a basis for their strategy. The Philippines is more conscious of their current issues and giving stronger advice to change the situation. On the other hand, Indonesia is spending a long time defining the roles of each body and explaining that each policy of

[124] Indonesia Pedoman Pertahanan Siber (2014)

[125] DICT National Cyber security Plan 2022 (2016)

the government should follow these guidelines. The Indonesian strategy is going back forth between recommendations and how to implement them and in which order. They are also lacking the proactive approach which is highly necessary. In comparison, the Philippines have a much clearer and much more complete strategy.

The two countries also have different focuses. The scope of the Philippines is larger but still not enough because, as presented in the literature, having a good cyber security requires far more investment than what both countries are currently making, whether it is in terms of money, workforce, knowledge, education, and culture.[126]

B. Strategic Factor

I will now analyse the strategy of Indonesia, through the motivation, the approach they had to it, the strategy making in itself and the content, to try and understand whether it is positive or negative for the improvement of cyber security.

a. Strategy Motivation Analysis

Why did Indonesia decide to make its first cyber strategy? What were the motivations behind this choice? The country, as I have explained earlier, did not find the topic of cyber security very important before 2014. They were not publicly reacting when a cyberattack was happening in the country. In this case, I believe the realist and the constructivist traditions can both partially explain the shift in the Indonesian motivation. I will also compare it with the Filipino motivation.

According to Seuring and Muller, cyber security is difficult to establish for developing countries. Those difficulties lie into the "institutional stability,

[126] The Asia Foundation (2022)

building knowledge, legal framework and private sector engagement".[127] Cyber security in Indonesia was barely existing before Joko Widodo launched the writing of the first strategy. The constructivist theory can explain why this threat was not interesting enough for the leader of the country, Susilo Bambang Yudhoyono (SBY). A part of this theory is about identities, preferences, and interests. If I take the constructivist idea that identity and interest shape the politics that are going to be launched, I have found that neither Susilo Bambang Yudhoyono (SBY) nor Joko Widodo had particular interest in cyber security. There is almost no information on cyber politics under SBY presidency. This corroborates the points made by constructivists that if the decision maker has no interest in a topic, they are not going to take care of it. Furthermore, Indonesia also had other issues at the time. When other countries were dealing with their cyber strategies, Indonesia had terrorism with the Bali bombings in 2002.[128]Aceh province was trying to obtain its independence until a tsunami hit its land in 2004.[129] Indonesia was also trying to negotiate with them until 2006. In 2009, there was also two massive earthquakes in Sumatra[130] and in West Java[131]. SBY was more trying to achieve stability for the country[132], being the first elected president and after having had a dictator for 30 years and three presidents in five years.[133]

However, if the leaders' interests were not a reason why they were motivated to publish a cyber strategy, norms and beliefs could be a good

---

[127] Seuring et Müller (2008)

[128] Gunaratna (2012)

[129] Braithwaite *et al.* (2010)

[130] Earthquake - Sumatra, Indonesia | Australian Disaster Resilience Knowledge Hub (2009)

[131] 2009 Indonesia (West Java) earthquake: CWS emergency appeal 10-05-09 - Indonesia | ReliefWeb, (2009)

[132] Aspinall (2015)

[133] ABC News (2014)

motivation to do it. Constructivists are explaining how norms and beliefs frame the actions of the actors, giving them an idea of what is possible to be done, what is appropriate and what is effective. The norm on having a cyber security strategy was set at the beginning of the 21st century. Many countries such as the US[134], France[135], and the UK[136] have participated in the creation and establishment of this norm. These countries published their first cyber security strategy between 2001 and 2005. For example, Winger showed similarities between the US and the Filipino' strategies. The Philippines produced a paper that was similar to the American one. This shows how the norm to have a cyber strategy shaped international politics, and how social reproduction pushed the Philippines to have a cyber strategy. When it comes to Indonesia, even though the international norm did not push them to have a cyber strategy as soon as other countries, they eventually came to have one, which shows that the norm injunction finally worked. I observe many reasons why Indonesia did not do it earlier. Firstly, compared to the Philippines, they did not have cooperation with the US. Secondly, as Muhammad Syaroni Rofii explained, Indonesia's perception of cyber threat is very low, which means that they did not assess that there was a risk at the time. Moreover, Ulum explained that this low perception created a poor cyber culture, which obviously delayed the creation of their cyber security strategy. The Philippines had their perception of risk way earlier, with the I LOVE YOU attack, and therefore they had their cyber strategy earlier. In the end, constructivists would argue that the norm of having a cyber strategy pushed Indonesia to do it too. However, it does not explain the delay. The realist tradition that could explain this better.

---

[134] *The National Strategy to Secure Cyberspace* (2003)

[135] *E-administration : du PAGSI au programme Action publique 2022* (2021)

[136] National Audit Office (2013)

Cyberattacks in Indonesia increased just after Joko Widodo became president, which made him unable to ignore the problem. However, in terms of interest and preferences, the constructivist's theory does not really apply. Joko Widodo has a degree in forestry engineering.[137] What pushed him to act on cyber security was the rising number of attacks and his defence minister who claimed that Indonesia was going to face a "cyber war".[138] Not only were they attacked a lot but in 2013, according to the company Akamai, Indonesia was also the first source of cyberattacks.[139] In 2014, according to Akamai again, they were the second source of attacks.[140] The reason why Indonesia was ranked that high is because computers in Indonesia were the victims of trojan horses which zombified them in order to use them in future attacks.[141]

This is when the realist tradition becomes of interest for this analysis. The realist tradition claims that states are living in an anarchic system. The cyber world is a "jungle", and international politics are described by realists the same way. There are no supranational rules or entities that are ruling over the cyber domain. This is the reason why malicious actors are using it to conduct their operations. Even though sometimes they get arrested by governments, most of the time they succeed in conducting their malicious activities. The cyber realm became "the fifth domain of battlefield", as put in the Indonesian White Paper, and states feel the need to protect their own interests.

Indonesia was motivated to create a cyber strategy because the cyberattacks were harming the national security and the interest of the country.

---

[137] Joko Widodo | Biography & Facts | Britannica (2023)

[138] Parameswaran (2015)

[139] WeLiveSecurity (2013)

[140] Jurriens and Tapsell (2017)

[141] Jurriens and Tapsell (2017)

Indonesia is trying to protect the "primacy of the nation states". The country tries to protect itself and its national interests with a cyber strategy. Secondly, they behave rationally: they recognize that cyberattacks are a threat to society and to their national security, therefore they are trying to put strategies and laws in place to protect their populations, their governmental entities. I am not assessing here their ability to do it but only the fact that they have indeed rationally tried to do it.

Lastly, the realist tradition speaks about the balance of power. This echoes with the "cyber war" evoked by the defence minister. The balance of power means that states will not start a war with others because it would lead to retaliation and, in the end, to mutual destruction. There are many types of cyber actors: cyber criminals, state sponsored groups, hacktivists, and all of them are trying to breach the national security of the country. These groups do not all have affiliations to countries. Some advanced persistent threats for example do not always have a clear link to a country, which means if they attack no one knows who to blame. Moreover, concerning the eventuality of a cyber war, there is some kind of balance of power, because Indonesia knows that it is yet to have the capabilities to fight in a cyber war and that the country is at the starting phase in terms of cyber security. Therefore, as the realist theory puts it, the country is rationally not going to put themselves in a position where it would lose a war, damage its security, and endanger its self-interest. This would also be a motivation for the country to create a cyber security strategy.

The motivation of the country is good as willingness to improve a situation is a first step to do so. However, it is not enough, and I will now evaluate the approach used in the strategy.

b. Strategy Approach Analysis

As explained in the strategy presentation and comparison, Indonesia is using almost only the active approach to cyber security. As shown in the

literature review, active approach corresponds to the NIST framework and to "identify, protect, detect, respond, recover".[142] Why did Indonesia choose this approach and barely spoke about the proactive approach to cyber security? Two approaches which have been explained in the theoretical framework, the risk management theory, and the constructivist tradition, can be applied to answer this question. I will also compare the Indonesian approach with the Filipino approaches.

Risk management theory helps to explain why Indonesia decided to use the NIST active approach. Indonesia had a lot of cyberattacks when the country elaborated its cyber strategy. It was the reason why the president Joko Widodo launched its creation. It seems then that it is the risk that made them write their strategy. In the strategy, they start by listing six objectives (detailed in the section VI A. a. of this dissertation), which is also coherent with risk management theory.[143] It presents the public who should follow the guidelines. Then, it quickly says that the Defence Ministry as well as the Indonesian army (TNI) should develop a process that can effectively evaluate the situation and facilitate its continuous improvement to mitigate future issues. However, the word "should" is a problem here. Indonesia asked for the procedure to be created but did not create it. Indonesia definitely used the risk analysis theory to elaborate its strategy. The only part of the risk management theory which is not covered is the economic control activity.

This theory explains well why Indonesia decided to use the NIST framework. The latter requests, in the first part "identification", to assess the risk and create a "risk management strategy" as well as to identify the "assets management" process and the "business environment". The second part, entitled

[142] Mylrea et al. (2017)

[143] Indonesia Pedoman Pertahanan Siber (2014)

"protect", deals with "awareness and trainings", "data security" or "maintenance". The third part, "detect", is about looking for the malwares to create a continuous process of detection. The fourth part, named "respond", is about "communication", "mitigation" and "improvement". The last part, "recover", is about having "recovery plannings". The NIST framework allows the country using it to "manage and reduce risks" linked to cyberattacks. It also helps to have "continuous improvement".[144] It is however a complement to a cyber strategy and not a strategy in itself. The framework is internationally recognized, and its good reputation would be a reason why Indonesia chose it.

This also recalls the constructivist theory, which explains that norms set what can be done, what is appropriate and what is effective. The NIST framework sets such a norm and therefore is of good use for a country who is trying to implement an effective cyber security. However, I am wondering why Indonesia is barely talking about proactive cyber security. The latter, as the Philippines puts it, refers to "defend", "deter" and "develop".[145] Defend is about improving the capabilities of a country so it can defend itself as well as improving the people's abilities and knowledge in cyber security. Deter is about investigating and preventing an attacker from conducting its malicious actions. Develop is improving the cyber security industry by investing in it.[146] I would argue that the lack of proactive approach in the Indonesian strategy is due to a lack of good technologies and lack of competent workers. Comparing the two countries' strategies, the two approaches of the Philippines are much more complete and try to have a larger scope of action. Their active and proactive approaches allow them to act when a cyberattack happens and before it even happens. Indonesia is trying to improve, but obtaining effective technology and

[144] Cybersecurity Framework Components (no date)

[145] DICT National Cyber security Plan 2022 (2016)

[146] THE "3D" NATIONAL CYBER SECURITY STRATEGY (2017)

educating people to cyber security takes time and investment. The strategy is partially trying to remediate this problem by creating training programs and by requesting the creation of better technological infrastructure. However, having only one approach to cyber security, as Fischer explained, is dangerous for organisations.[147]

Table 3: Comparison of the Indonesian and Filipino Approaches

	Indonesia	**The Philippines**
Active approach	Monitoring	Identification
	Prevent	Protect
	Analysis	Detect
	Defence	Respond
	Information Security Improvement	Recover
Proactive approach		Defend
	Counterattack	Deter
		Develop

The approach chosen by the Indonesian government is levelled with its capacities. They are trying to follow the norms followed by other nation states while managing the cyber risk with their approach. It is unclear why they have not chosen the NIST framework as a structure the same way the Filipino

[147] Fischer (2005)

government did even more so when they are naming it as a standard. I will now analyse the structure of their cyber strategy in the next section.

c. Strategy Structure Analysis

When I started reading both the Indonesian and the Filipino strategies, I realised how their structures were important to have an efficient strategy. I will now analyse the structure of the Indonesian strategy through the lens of the risk management theory and compare it with the Filipino strategy. A strategy written using the risk management strategy is based on the perceived cyber risks of Indonesia. It gathers "activities" to prevent "accidental loss". Finally, it uses the DRA framework to be able assess it and make it evolve.

Risk management theory can explain how both Indonesia and the Philippines have elaborated their strategies. The Indonesian strategy has five chapters and the Filipino, four.

The Indonesian first one is an introduction chapter which is defining the "objectives", "scope" and the laws and policies. The basis of the DRA is to start by defining the objectives, which Indonesia is doing at the beginning of their strategy. However, they also do it a second time detailing six clearer objectives in a part called cyber defence target.

The Indonesian second chapter deals with threat and attacks as well the current conditions of the policies, institutions, technologies, and human resources, and needs to improve these 4 categories. It is an important step in the risk management theory as it allows the strategy maker to have all the data in mind to create the best strategy.

The Filipino structure differs from the Indonesian one. They have as a second chapter the "scope", which encompasses the two first chapters of the Indonesian strategy. Then, the Philippines have a chapter on the "National

Strategic Context". This is a long chapter in which they explain their "vision", the "framework", "the risk management approach" and the "strategic collaboration". This part is encompassing a part of the Indonesian second chapter and their third chapter. It is clearer as each part is way much more delimited and they do not overlap on one another.

The Indonesian third chapter deals with the cyber defence key points. It presents the principles, targets, the roles, tasks, and functions of the TNI. This part is important but if I compare it with the Filipino strategy, it is a small part of their cyber strategy, and I am questioning here the interest of writing an entire chapter about it. These could be added to other parts of the strategy and avoid the repetition and the lack of clarity of having different parts dealing with objectives. There are also repetitions inside the parts themselves, between the target part and the function part, and the tasks, there are many repetitions of things to be done such as awareness or information availability. These parts are very important for cyber security. However, in terms of structure, it makes the strategy hard to read because the reader always has the impression to read almost the same things and the sections are not clearly defined nor framed.

Chapter four deals with the implementation of cyber security. It starts with larger requirements and with a framework for cyber defence implementation, then the stages of the implementation and then it presents the different phases. The strategy is again taking its four focus points, "policies", "institutions", "technology", and "human resources", to frame where their actions should be taken and what they should be. The strategy has an entire part dedicated to risk management and assessment and nine pages are allocated to it.

The second part of this chapter speaks about the stages of cyber defence, which is about giving the actions that should be taken. Finally, the third part is about explaining in which order the actions should be taken. I have found two

problems. Firstly, the recommendations in the stages of cyber defence are mixed between the technology's recommendations, the human resources' recommendations, the policies' recommendations, and the institutions' recommendations. It makes it difficult to know as a reader which part is relevant for you, and which is not. The second problem is the fact that the recommendations are not already in order. As a reader you do not know where to start when you read the recommendations and you need to read the next section to be able to know. It loses the reader and shows a lack of clarity in the strategy.

This part corresponds to the Filipino fourth chapter on "key strategic initiative". They present their "key programs areas" with 4 different focuses on "critical infrastructure", "government networks", "supply chain" and "individuals". These parts are presenting the recommendations in order. Then, the strategy deals with the approaches the Filipino cyber security should observe. Compared to the Indonesian one, it is not giving more recommendations in the approaches part and has already given it in order so there is no need to redo it.

If I take the requirements for risk management theory, the identification and the measurement were clearly respected as the Indonesian and the Filipino documents have an entire part on risk assessment, however economic control is not talked about in the Indonesian document. Concerning the Deeming circle and "Plan, Do, Check, Act", on one hand, the document is saying that the army and the Minister of Defence should have an assessment plan to monitor their systems and correct the errors. However, this only concerns systems and not the rest of the strategy. On the other hand, the risk management approach of the Philippines concerns all parts of their strategy.

The structure of the cyber security strategy of Indonesia is respecting almost all the requirements of a good cyber strategy framework according to Fischer.[148] It has almost everything, "goals, strategies, policies, procedures and personnel", except for "extent of problems and perceptions". It is, however, quite complex, which makes it difficult to read. It goes back and forth between sections and is repetitive. The recommendations they are giving are not put by sectors and the strategy is also not giving recommendations in order. They dedicated an entire section to said recommendations, presenting them and then repeating them in order, when they could prevent confusion just by writing them once in order. They dedicated an entire section to said recommendations, presenting them and then repeating them in order, when they could prevent confusion just by writing them once in order. They started to work with the risk management theory, however it seems like they have not used it fully to write their strategy. In comparison, the Filipino strategy is easy to read as it is very clear. It has all the requirements of Fischer's framework. Recommendations are by sector and in order. It is easier to implement this strategy as its recommendations are clearer and more accessible.

d. In Depth Analysis of the Content

Now that I have analysed the motivation, the approach, and the structure, I will analyse the content of the strategy. I will use the literature review on effective cyber security, the comparison with the Filipino strategy and the different traditions and theory to assess the content of the Indonesian cyber security strategy.

The first part of the content that I want to analyse is to whom the cyber strategy is destined to. In the Indonesian case, the cyber strategy is for the Ministry of Defence and the TNI. In my opinion, this is already a problem,

[148] Fischer (2005)

because a cyber strategy should be destined not only to the Defence Ministry and the army but also to all governmental entities, so that everyone is involved in the process. It highly reduces the scope of action to enforce the strategy outside of these two organisations. Making the cyber defence of Indonesia only the responsibility of these two entities is creating vulnerabilities in all the other Indonesian governmental entities. Comparatively, the strategy of the Philippines is for all the public and private entities, the "civil society", universities and private people. In terms of scope, Indonesia is putting in their scope the "definition" and laws, the "target" and type of threats, the "needs" and the implementation stages. The Philippines is much more practical. They are talking about all networks in the Philippines, the "hardware and software" and adding norms and standards to be respected.

In terms of presenting the objectives to attain, Indonesia, as I explained before, is doing it twice. In the first part, they are giving larger objectives such as "strengthening the national defence", developing and establishing their cyber defence. These objectives are in line with the realist tradition. By expressing their will to improve their national defence, they are clearly putting their national interest first, and trying to improve their position in the balance of power on the international scene. The objectives of their Filipino counterparts are much more specific from the beginning. They are about protecting critical infrastructure, being cyber resilient, having coordination between various organisations, and educating the Filipinos.

Indonesia then expresses objectives in the target part, which are more specific. These are more related to my literature review on effective cyber security and resembling the Filipino goals. They are about identifying and understanding the threats and risks, raising awareness, and having a good infrastructure, set of skills and knowledge to implement the strategy. These are the three goals that are in line with what the authors of my literature review are

requesting for effective cyber security. There are three other objectives which are about involving the TNI and the Ministry of Defence. This target audience is important, but as explained in the first section, it is not large enough. Then, there is the "expansion of resources to develop the cyber defence of Indonesia as a part of the national defence". This is a very vague and unclear part, as no one can know which resources need to be developed. The last objective is the elaboration of deterrence, action, and recovery strategies. This is interesting as it is more part of the proactive approach. However, we have observed in previous parts that Indonesia is barely having this approach in their strategy. This means that they have objectives in their strategy that they do no back up with propositions in their plan.

I will now assess their plan using the risk management theory and the literature review. Their framework starts with all the policies they want to respect, and the risk management framework they want to implement. Then the theory presents the technology and infrastructure requirements, which are larger objectives discussed later, and finally it introduces the human resources' part. These are in line with what Elkhannoubi and Bellaissaoui are requiring – an organisational pillar, a legal pillar, and a technological pillar. Indonesia is even adding one more with the human resources part.

The part on policies is important as explained by Fischer. Then, in their framework, they discuss the assessment and improvement of information security management. They also mention how audits will be conducted, how the risk will be assessed and determine if an immediate solution is necessary or not. These are in line with the literature gathered, as well as with the risk management theory. Indonesia's technological part is setting the larger requirements needed and then the human resources requirements. The human resources' part is very important as it is requiring all the different up to date training to have competent workers. This is in line with Elkhannoubi and

Belaissaoui recommendations. However, in this part there is no injunction to create a higher education degree. The strategy only deals with training for workers, while the Filipino one was demanding the creation of some university degrees. The Filipino framework is different, it bases itself on the NIST pillars and then presents the agencies and their roles in the cyber defence. It also presents the target audience of the strategy, which are the "public, private, and international partners".

The Indonesian strategy continues with the actual recommendations, which are ordered by stages but not by order of what should be done first. Their prevention stage is about having a secured architecture, having security policies, having human resources security with background checked personnel. These are in line with what Srinivas et al. is requiring. However, if the requirements of the strategy are talking a lot about the human part which was necessary according to Srinivas et al., there are no requirements on the time component. This strategy never gives time constraint for it to be implemented, which creates a never-ending issue that might or might not be patched someday. The Filipino strategy, however, deals with compliance, having training for citizens and cyber security professionals. It has a time component, as the Philippines have written their strategy for 2022. It also has parts on how to protect networks. This shows how they are more advanced than Indonesia, as they are talking about protecting the architecture and not creating it.

The Indonesian information security monitoring stage is about keeping the availability, integrity, and confidentiality of data intact. This is recommended by Srinivas et al. to have good cyber security. However, Srinivas et al. is also recommending "authentication" rules, "authorization" rules, rules to prevent the "physical theft of devices", rules to prevent "non-repudiation" and finally to keep the "freshness" of data. All these rules are not tackled in the Indonesian strategy. The Filipino strategy has in comparison considered

"Information Security" a "key area for cyber security" and they are mentioning all the requirements.

In the analysis stage, the Indonesian strategy goes back to implementing a secured architecture, but also goes further to analysing malwares and implementing investigation forensic to keep the integrity. This part should be talking about the MITRE ATT&CK framework, as it helps in analysing attackers' behaviour. It would have been clearer and more straight to the point if they had incorporated the framework they will use. The Filipino strategy is going further, with the establishment of a department of cyber "threat intelligence" and "analysis".[149] However, they are not talking about the MITRE framework, on that part, their strategy is not going as deep as the Indonesian one.

In the Indonesian defence stage, the strategy deals with detection and recovery stages. It is talking about the different threats they could find. It is also talking about the next steps to be taken in case of an attack, in terms of diplomacy and laws, and with other organisations when it comes to counterattacking. These stages – recovery and detection – are two stages from the NIST framework. They are important; however, they need to be correlated with all the other parts of the framework. It is an issue because they are not clearly using the standard. Moreover, using it only halfway makes it half efficient and therefore, it creates vulnerabilities. In comparison, the Filipino strategy is using both approaches fully.

The next part is about counterattacking, which they claim to consider carefully from a legal and diplomatic standpoint. It is a repetition from what they had previously said in the defence stage. They are giving some of the counterattack possibilities. In this case, it is clear that they are trying to show

[149] DICT National Cyber security Plan 2022 (2016)

their strength to potential threat actors. However, this part has no recommendations in it. For the Philippines, they explain that their deter part goes with the protection of critical infrastructure and the three recommendations on compliance, regular cyber exercise and having a "national database for monitoring and reporting".

The last part of the Indonesian strategy is about improvements, in which they recommend using the risk assessment part to improve it. It shows again how they repeat themselves. The Filipino strategy does not have a part on improvement, as it is already talking about "plan do check act" and risk management theory.[150]

In the next section, Indonesia finally gives the order on which action should be done first. Each part has an output section after it. The Philippines do not have any part such as this one, because their recommendations are already in order and by sector.

They start with the road map and policies. Then, the maturation stage is about the establishment of institutions and audits to check if the Ministry of Defence and TNI are respecting the previous policies. They also talk about recruitment and technology, and implementing risk based IT security technology. At the utilisation stage, they speak about improving the first policies of the maturation stage with new standards such as ISO 27001. They also start talking about international cooperation. Finally, the optimization part deals with participating in cyber competitions, developing cyber defence, and having security risk assessment run by a third party.

This part has a lot of different problems. Firstly, the strategy is not clear. Compared to the Filipino one, it is obvious that the structure is very problematic.

[150] DICT National Cyber security Plan 2022 (2016)

It is difficult, as a decision maker, to make these decisions when every part is giving different recommendations on the actions to be taken. There are the framework recommendations, the stages of defence recommendations, the phasing of defence recommendations. Every one of them are good recommendations, but the way they are written makes it very difficult to know where to start and what to do first.

Moreover, there are plenty of other issues. Diverse authors had previously evaluated them such as Mulyadi and Rahayu who talk about the lack of private public partnership and the lack of cooperation.[151] This is an issue that is tackled in the Filipino strategy. Another problem I have found looking at the Indonesian strategy is the lack of requesting tailored cyber organisations. This had been pointed out by Al Mehairi et al. who explained that it is necessary to have good cyber security.[152]

In conclusion, the Indonesian strategy is overall based on good points, however, it is way too detailed on some parts that should be dealt with later. There are also many structural problems and a lack of clear and chronologically organised measures to actually apply this cyber security plan. Moreover, even in the part of the strategy that is supposed to be the chronological plan, the Indonesian strategy is difficult to implement as the decision maker does not know if they should prioritise the plan or start with the recommendations made in the previous part. Thanks to all the authors, traditions, and theory, I have pointed out that there are many parts of the strategy that could be improved and many problems that should be addressed. Nevertheless, this strategy has been published to create a framework which was before inexistant. The comparison with the Filipino strategy shows how the Philippines are more mature than

[151] Mulyadi and Rahayu, D. (2018)

[152] Al Mehairi et al. (2022)

Indonesia in terms of cyber security. A strategy is supposed to pave the way to improve a certain domain and if it is flawed, improvement becomes difficult and instead stagnation becomes the norm. Indonesia needs to restructure and rethink its theory to make it more accessible, and implementable.

VII. Conclusion

This dissertation has changed a lot since the beginning of its writing. The factors have changed as well as the structure. It started with two potential paths. There was one path in which Indonesia and the Philippines had the same reaction and one in which the two countries were behaving differently. These reactions were supposed to show me if I was going to study both strategies as a factor of their cyber stagnation or if I had to focus on the Indonesian cyber strategy. This dissertation has shown that the two countries had different reactions and that I had to concentrate myself on the Indonesian cyber strategy. Using three traditions and theories, the literature review, and the Filipino cyber strategy, I analysed the Indonesian cyber strategy at different levels. I studied their motivation, the approaches they used, the structure and the content of their cyber strategy.

During this dissertation, I noticed that the Indonesian cyber strategy was making some good points but also had many problems. These good points are backed up by many authors, which shows how cyber security should theoretically improve. They firstly have the motivation to improve things. They passed many laws and published several policies. They are also recommending numerous directives in their strategy, such as having secured infrastructure, or improving their digital investigation. However, numbers and reactions show how cyber awareness and cyber security are still not fulfilled in Indonesia, even though their strategy was published in 2014.

Problems remain in the Indonesian strategy, and I identified them as follows. Firstly, the document does not target the whole country but only a few bodies (Defence Ministry and TNI). Secondly, the approach chosen by the Indonesian Ministry of Defence is incomplete. Thirdly, its implementation is flawed by its structure and the constant repetitions within the strategy. Fourthly, there are plenty of missing points in the content, such as the lack of private

public partnership, international cooperation, or information security. All these issues, whether they are in the strategy or lacking from it, are refraining Indonesia to have a good cyber security. This makes the Indonesian cyber strategy responsible for the country's stagnation at a cyber level.

However, one can wonder if there are other limits that could be taken into consideration and could also stop Indonesia from having a better strategy. I have identified other factors which are the economic factor, the technological factor, the political factor, the cultural factor, and the time factor.

The economic factor refers to the lack of financial investment Indonesia is putting into cyber security. The technological factor is the lack of technological advancements and the lack of educational training to use them. Indonesia does not have many university degrees in cyber security. The political factor would be the current laws of the country. Indonesia has recently passed a data protection law which is highly criticised. The cultural factor would be the way Indonesians perceive the importance of cyber security in their lives. I would also include that the structural differences in the Indonesian and Filipino strategies could be explained by their cultural particularities and by the organisational structure of their respective governments. Finally, the time factor is probably one of the most important. It refers to the necessary time to implement such a strategy, review it, correct it, and improve the situation. If you check the first Filipino strategy for example it is highly different from their second strategy, but they had the time to correct their mistakes and improve their situations. Indonesia has not had the time to take a step back and reflect on their situation after their first cyber strategy.

Based on the assessment of this dissertation, the strategy is definitely a factor that is stopping Indonesia to improve their cyber security. However, other

papers should be written to analyse the other factors and check their implication within the cyber security stagnation of Indonesia.

This research has a goal to understand if the cyber strategy of Indonesia is responsible for their bad cyber security. This dissertation could be used to point out the problems in the previous strategy and improve the following one.

A good strategy would help the Indonesian government to be more secure, as well as the whole Indonesian society. A broader implication of this research is that if Indonesia is not changing anything to its cyber strategy, attacks will continue to increase as it has been the trend for the past years. This will taint Indonesia’s reputation as a non cyber secured country, which will have an impact on other sectors.

The economic sector will be impacted, since cyberattacks are expensive for companies. They are extremely problematic for customers' privacy. Not having a good cyber security strategy or good laws on data protection prevent foreign companies who are concerned with their customer’s privacy from settling down in Indonesia. Besides their reputation and privacy, it hurts the economy of the country as investors will refuse to invest in unsecured companies.

Individuals are also the victims of these attacks. There is definitely an economic component to cyberattacks targeting the Indonesian population, but not only. There is also a data problem, which is followed by privacy issues. If cyberattacks continue to happen and their results get sold on the dark web, it would be logical that identity theft will become more common. Indonesian people already suffered from attacks in which their data were stolen, and their credit cards used to purchase things they had never authorised.

Not having good cyber security also impacts the national security of the country. When an APT is able to steal sensitive data from the intelligence service of Indonesia or from any minister, it is highly possible that they also stole documents related to national security. This creates a major risk for a country who already is involved in territorial conflict with China.

Indonesia must revise its strategy and start cooperating with countries that are more cyber secured, to improve their own capacities. This dissertation has shown how Indonesia cyber strategy is responsible for the stagnation of its cyber capabilities. It has also shown that the cyber strategy is largely responsible for the non-consideration of cyber security as a major security concern in the country. The problems previously evoked prevent the country and its officials from implementing a good cyber security strategy.

I. Bibliography

ABC News (2014) 'Indonesia votes: From Sukarno to SBY', 21 April. Available at: https://www.abc.net.au/news/2014-04-22/an-indonesia-presidents-timeline/5379864 (Accessed: 16 June 2023).

Acanerler, A. (2021) *Top 5 Cyber Attacks in the Asia Pacific (APAC) in 2021*, *SOCRadar® Cyber Intelligence Inc.* Available at: https://socradar.io/top-5-cyber-attacks-in-the-asia-pacific-apac-in-2021/ (Accessed: 19 July 2023).

'Addressing the Lack of Cybersecurity Workforces in Indonesia : Center for Digital Society' (no date). Available at: https://cfds.fisipol.ugm.ac.id/2019/08/25/addressing-the-lack-of-cybersecurity-workforces-in-indonesia/ (Accessed: 19 July 2023).

Agustini, P. (2021) 'Kominfo Bantu Tangani Peretasan 10 Jaringan K/L Berdasarkan PP PSTE', *Ditjen Aptika*, 14 September. Available at: https://aptika.kominfo.go.id/2021/09/kominfo-bantu-tangani-peretasan-10-jaringan-k-l-berdasarkan-pp-pste/ (Accessed: 30 June 2023).

Alimpuangon, L.S. and Reyes, A.R.L. (no date) 'A Cybersecurity Awareness among Senior High School Students: A Descriptive Analysis'.

Anjani, N.H. (2021) 'Cybersecurity Protection in Indonesia', p. 13.

antaranews.com (no date) *BSSN records decrease in cyberattacks in 2022*, *Antara News*. Available at: https://en.antaranews.com/news/270015/bssn-records-decrease-in-cyberattacks-in-2022 (Accessed: 13 May 2023).

Aspinall, E. (2015) 'Stability and stagnation under SBY', *New Mandala*, 30 July. Available at: https://www.newmandala.org/stability-and-stagnation-under-sby/ (Accessed: 16 June 2023).

Aulianisa, S.S. and Indirwan, I. (2020) 'Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in

Indonesia', *Lex Scientia Law Review*, 4(1), pp. 31–45. Available at: https://doi.org/10.15294/lesrev.v4i1.38197.

Ayman Falak Medina (2020) *Indonesia's Palapa Ring: Bringing Connectivity to the Archipelago*, *ASEAN Business News*. Available at: https://www.aseanbriefing.com/news/indonesias-palapa-ring-bringing-connectivity-archipelago/ (Accessed: 6 May 2023).

Bedell, C. (no date) *What Is a Computer Worm and How Does It Work?*, *Security*. Available at: https://www.techtarget.com/searchsecurity/definition/worm (Accessed: 17 May 2023).

Beyer, R.E. and Brummel, B.J. (no date) 'Implementing Effective Cyber Security Training for End Users of Computer Networks'.

bferrite (2021) *Check Point Research: Asia Pacific experiencing a 168% year on year increase in cyberattacks in May 2021*, *Check Point Blog*. Available at: https://blog.checkpoint.com/security/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/ (Accessed: 19 July 2023).

Bhunia, P. (2017) 'Department of Information and Communications Technology Philippines releases National Cybersecurity Plan 2022 - OpenGov Asia', 27 October. Available at: https://opengovasia.com/department-of-information-and-communications-technology-philippines-releases-national-cybersecurity-plan-2022/ (Accessed: 19 July 2023).

Bigo, D. (2002) 'Security and Immigration: Toward a Critique of the Governmentality of Unease', *Alternatives: Global, Local, Political*, 27(1_suppl), p. 63.

BIN Denies Their Server Was Hacked By Chinese: It Is Under Control (no date). Available at: https://voi.id/en/news/85187 (Accessed: 30 June 2023).

‘Bjorka alleged to be behind the passport data leak of 34 million Indonesians’ (2023) *OBSERVER*, 6 July. Available at: https://observerid.com/bjorka-alleged-to-be-behind-the-passport-data-leak-of-34-million-indonesians/ (Accessed: 18 July 2023).

‘Björka’s Effective Hacktivism and Lessons for Indonesia – Stratsea’ (no date). Available at: https://stratsea.com/bjorkas-effective-hacktivism-and-lessons-for-indonesia/ (Accessed: 19 July 2023).

Bonnes pratiques (no date) *ANSSI*. Available at: https://www.ssi.gouv.fr/particulier/bonnes-pratiques/ (Accessed: 19 July 2023).

BOTEZATU, B. (no date) *LuminousMoth – PlugX, File Exfiltration and Persistence Revisited*, *Bitdefender Labs*. Available at: https://www.bitdefender.com/blog/labs/luminousmoth-plugx-file-exfiltration-and-persistence-revisited/ (Accessed: 18 July 2023).

Boucher, P. (2022) ‘Nouvelle édition de la norme ISO27002, version 2022’, *Medium*, 18 February. Available at: https://medium.com/@btk667/nouvelle-%C3%A9dition-de-la-norme-iso27002-version-2022-13387571e6c5 (Accessed: 19 July 2023).

Braithwaite, J. *et al.* (2010) ‘Aceh’, in *Anomie and Violence*. ANU Press (Non-truth and Reconciliation in Indonesian Peacebuilding), pp. 343–428. Available at: https://www.jstor.org/stable/j.ctt24hf62.12 (Accessed: 15 June 2023).

Bresnahan, E. (no date) *What Are the Benefits of the NIST Cybersecurity Framework*. Available at: https://www.cybersaint.io/blog/benefits-of-nist-cybersecurity-framework (Accessed: 18 July 2023).

Brown, C. and Eckersley, R. (2018) *The Oxford Handbook of International Political Theory*. Oxford University Press.

Candido, D. (2022) ‘Qu’est-ce que la norme ISO 27002:2022’, *Interfacing Technologies Corporation*, 7 September. Available at:

https://www.interfacing.com/fr/quest-ce-que-iso-27002-isms (Accessed: 19 July 2023).

CERT-PH (no date) *Advanced Persistent Threat Group, LuminousMoth Targeting Government Organizations from the Philippines | NCERT*. Available at: https://www.ncert.gov.ph/2021/07/15/advanced-persistent-threat-group-luminousmoth-targeting-government-organizations-from-the-philippines/ (Accessed: 9 July 2023).

Chen, E. (no date) *As Cyber Threats Grow, Indonesia's Data Protection Efforts Are Falling Short*. Available at: https://thediplomat.com/2022/06/as-cyber-threats-grow-indonesias-data-protection-efforts-are-falling-short/ (Accessed: 19 July 2023).

Choucri, N. and Clark, D.D. (no date) *Cyberspace and International Relations_ The Co-Evolution Dilemma-MIT Press (2019).pdf*, *Google Docs*. Available at: https://drive.google.com/file/d/1UxIww3ReO8lxxJQBW2k5U5JrfmI-9r8v/view?usp=embed_facebook (Accessed: 19 July 2023).

Cimpanu, C. (no date) *Indonesian intelligence agency compromised in suspected Chinese hack*. Available at: https://therecord.media/indonesian-intelligence-agency-compromised-in-suspected-chinese-hack (Accessed: 30 June 2023).

Ciolan, I.M. (2014) 'DEFINING CYBERSECURITY AS THE SECURITY ISSUE OF THE TWENTY FIRST CENTURY. A CONSTRUCTIVIST APPROACH'.

Clay, J. (2022) *Cyber Risk Index 1H'22 Snapshot*, *Trend Micro*. Available at: https://www.trendmicro.com/fr_fr/research/22/k/cyber-risk-index-1h-22-snapshot.html (Accessed: 19 July 2023).

Correspondent, L.Y. (2022) 'Indonesia hunts for Bjorka, hacker selling 1.3b SIM card users' data, taunting officials', *The Straits Times*, 18 September. Available at: https://www.straitstimes.com/asia/se-asia/indonesia-hunts-for-

bjorka-hacker-selling-13b-sim-card-users-data-taunting-officials (Accessed: 19 July 2023).

Poret, C. (2022) *ISO 27002 : 2022 – Qu'est-ce qui a changé ?*, *Feel Agile*. Available at: https://feelagile.com/iso-27002-2022-quest-ce-qui-a-change/ (Accessed: 19 July 2023).

Crockford, G.N. (1982) 'The Bibliography and History of Risk Management : Some Preliminary Observations', *The Geneva Papers on Risk and Insurance*, 7(23), pp. 169–179.

CSP-CERT® | Cyber Security Philippines - Computer Emergency Response Team® (no date). Available at: https://www.cert.ph/ (Accessed: 25 April 2023).

Cyber-criminalité : l'Indonésie est devenue le paradis des hackers - Le Parisien (no date). Available at: https://www.leparisien.fr/economie/cyber-criminalite-l-indonesie-est-devenue-le-paradis-des-hackers-21-10-2013-3245889.php (Accessed: 19 July 2023).

Cyberlands (no date) *Top 10 Cybersecurity Breaches in Indonesia*. Available at: https://www.cyberlands.io/topsecuritybreachesindonesia (Accessed: 14 May 2023).

Cybersecurity (no date) *e-Governance Academy*. Available at: https://ega.ee/cybersecurity/ (Accessed: 19 July 2023).

Cyberspace as the New Domain for Great Power Competition: Strengthening the Philippines' Cyber Capability in a Complex Security Environment - NDCP (no date). Available at: https://www.ndcp.edu.ph/cyberspace-as-the-new-domain-for-great-power-competition-strengthening-the-philippines-cyber-capability-in-a-complex-security-environment/ (Accessed: 19 July 2023).

Dash, B. and Ansari, M.F. (2022) 'An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy', 09(04).

De Ramos, N.M. and Esponilla Ii, F.D. (2022) 'Cybersecurity program for Philippine higher education institutions: A multiple-case study', *International*

Journal of Evaluation and Research in Education (IJERE), 11(3), p. 1198. Available at: https://doi.org/10.11591/ijere.v11i3.22863.

Demboski, M. (no date) *APAC's vulnerability to cyber attacks*. Available at: https://www.ironnet.com/blog/apacs-vulnerability-to-cyber-attacks (Accessed: 19 July 2023).

Detros, K. (2022) 'Using Data to Protect Data: Addressing Gaps in Cyber Threat Reporting in the Philippines', *Tech For Good Institute*, 21 August. Available at: https://techforgoodinstitute.org/blog/expert-opinion/using-data-to-protect-data-addressing-gaps-in-cyber-threat-reporting-in-the-philippines/ (Accessed: 19 July 2023).

DICT (2016) *National Cybersecurity Plan 2022*. Available at: https://www.dict.gov.ph/wp-content/uploads/2017/04/FINAL_NationalCyberSecurityPlan2022.pdf (Accessed: 20 March 2023).

DICT (no date) *DICT-Philippines-Cybersecurity-Strategy-compressed*. Available at: https://www.bmap.net/wp-content/uploads/2019/03/DICT-Philippines-Cybersecurity-Strategy-compressed.pdf (Accessed: 19 July 2023).

Duterte's controversial legacy: Making Philippine strongmen 'cool' (no date) *Nikkei Asia*. Available at: https://asia.nikkei.com/Politics/Duterte-s-controversial-legacy-Making-Philippine-strongmen-cool (Accessed: 19 July 2023).

E-administration : du PAGSI au programme Action publique 2022 (2021) *vie-publique.fr*. Available at: http://www.vie-publique.fr/eclairage/18925-e-administration-du-pagsi-au-programme-action-publique-2022 (Accessed: 12 June 2023).

Earthquake - Sumatra, Indonesia | Australian Disaster Resilience Knowledge Hub (2009). Available at: https://knowledge.aidr.org.au/resources/earthquake-sumatra-indonesia/ (Accessed: 15 June 2023).

Elkhannoubi, H. and Belaissaoui, M. (2015) 'A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification', in *2015 15th International Conference on Intelligent Systems Design and Applications (ISDA)*. *2015 15th International Conference on Intelligent Systems Design and Applications (ISDA)*, pp. 1–6. Available at: https://doi.org/10.1109/ISDA.2015.7489156.

Eriksson, J. (no date) *The Information Revolution, Security, and International Relations_IR relevant Theory.pdf*, *Google Docs*. Available at: https://drive.google.com/file/d/1rYts0wfGqwpG5VByq3tHaOk8_Nfhk6cJ/view?usp=embed_facebook (Accessed: 19 July 2023).

ETTelecom (no date) *Data breach in networks of Indonesian ministries and agencies - ET Telecom*, *ETTelecom.com*. Available at: https://telecom.economictimes.indiatimes.com/news/data-breach-in-networks-of-indonesian-ministries-and-agencies/86253229 (Accessed: 30 June 2023).

Farrell, T. (2002) 'Constructivist Security Studies: Portrait of a Research Program', *International Studies Review*, 4(1), pp. 49–72. Available at: https://doi.org/10.1111/1521-9488.t01-1-00252.

Fathan Taufik, A. (2021) 'Indonesia's cyber diplomacy strategy as a deterrence means to face the threat in the indo-pacific region', *Journal of Physics: Conference Series*, 1721(1), p. 012048. Available at: https://doi.org/10.1088/1742-6596/1721/1/012048.

Fischer (2005) *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. Available at: https://apps.dtic.mil/sti/pdfs/ADA463076.pdf (Accessed: 24 May 2023).

Get to Know Ransomware Attacks (2022). Available at: https://mycarrier.telkom.co.id/article/get-to-know-ransomware-attacks (Accessed: 13 May 2023).

Ghernouti-Hélie, S. (2010) 'A National Strategy for an Effective Cybersecurity Approach and Culture', in *2010 International Conference on Availability,*

Reliability and Security. 2010 International Conference on Availability, Reliability and Security, pp. 370–373. Available at: https://doi.org/10.1109/ARES.2010.119.

Ghifari, D. (2022) *'I think Indonesia's cybersecurity is run by 14-year olds': hackers - Science & Tech - The Jakarta Post*. Available at: https://www.thejakartapost.com/culture/2022/09/01/i-think-indonesias-cybersecurity-is-run-by-14-year-olds-hackers.html (Accessed: 13 November 2022).

'Global Cybersecurity Index 2017' (no date).

Gomez, M.A. (2023) *Tracing strategic preferences in cyberspace: The role of regional and domestic strategic culture*. Available at: https://www.tandfonline.com/doi/epdf/10.1080/01495933.2022.2111912?needAccess=true&role=button (Accessed: 11 April 2023).

Gonzales, A. (2022) '69% of PH organizations experienced ransomware attacks in 2021 – Sophos', *RAPPLER*, 6 May. Available at: https://www.rappler.com/technology/philippines-ransomware-attacks-2021-sophos-report/ (Accessed: 19 July 2023).

GOV Indonesia (ed.) (2008) *Buku putih pertahanan Indonesia, 2008: disahkan dengan Peraturan Menteri Pertahanan, Republik Indonesia nomor PER/03/M/II/2008 tanggal 18 Februari 2008*. Cet. 1. Jakarta: Departemen Pertahanan, Republik Indonesia.

GOV Indonesia (2014) *Pedoman Pertahanan Siber*. Available at: https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf (Accessed: 21 February 2023).

GOVPH (2005) *Philippines 2005 National Cyber Security Plan 2005*. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Philippine_2005

_National%20Cyber%20Security%20Plan%202005.pdf (Accessed: 12 June 2023).

GOVPH (2022) *Republic Act No. 10175 | GOVPH*, *Official Gazette of the Republic of the Philippines*. Available at: https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/ (Accessed: 28 March 2023).

Griffiths, J. (2020) *'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on | CNN Business*, *CNN*. Available at: https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html (Accessed: 18 July 2023).

Gulla, V. (2023) *3,000 'high level' cyberattacks in PH in 2022: DICT*, *ABS-CBN News*. Available at: https://news.abs-cbn.com/business/04/12/23/3000-high-level-cyberattacks-in-ph-in-2022-dict (Accessed: 19 July 2023).

Gunaratna, R. (2012) 'Ten Years after Bali', *Counter Terrorist Trends and Analyses*, 4(10), pp. 2–6.

Heinl, C.H. (2014) 'Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime', *Asia Policy*, (18), pp. 131–160.

Hope, A. (2023) *34 million Indonesian Passports Exposed in a Massive Immigration Directorate Data Breach*, *CPO Magazine*. Available at: https://www.cpomagazine.com/cyber-security/34-million-indonesian-passports-exposed-in-a-massive-immigration-directorate-data-breach/ (Accessed: 19 July 2023).

https://thecyberexpress.com (2023) 'Imigrasi Cyber Attack: 34 Million Passport Records Stolen', 5 July. Available at: https://thecyberexpress.com/imigrasi-cyber-attack-bjorka-passport-records/ (Accessed: 18 July 2023).

ID-SIRTII/CC (no date). Available at: https://idsirtii.or.id/en/bssn_page.html (Accessed: 19 July 2023).

Ikhwan, H. (no date) *Server Intelijen dan 10 Kementerian Kabarnya Diretas Hacker Tiongkok, BIN Membantah*. Available at: https://www.vice.com/id/article/y3d7nm/bin-membantah-laporan-servernya-diretas-kelompok-hacker-mustang-panda-asal-tiongkok (Accessed: 30 June 2023).

Indonesia hunts down Bjorka as hacking spree could be 'tip of the iceberg' (2022) *South China Morning Post*. Available at: https://www.scmp.com/week-asia/politics/article/3192562/indonesia-hunts-down-bjorka-analysts-warn-hacking-spree-could-be (Accessed: 19 July 2023).

International Telecommunication Union (no date a) 'Global Cybersecurity Index 2017', p. 78.

International Telecommunication Union (no date b) 'Global Cybersecurity Index 2020', p. 172.

Interpol (2021) 'ASEAN CYBERTHREAT ASSESSMENT'. Available at: https://www.interpol.int/en/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf.

Irene Christine, D. and Thinyane, M. (2020) 'Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries', in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pp. 71–78. Available at: https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00027.

Irnasya, S. (no date) 'Analyzing Indonesia's National Cybersecurity Strategy : Center for Digital Society'. Available at:

https://cfds.fisipol.ugm.ac.id/2021/07/28/analyzing-indonesias-national-cybersecurity-strategy/ (Accessed: 19 July 2023).

Janti, N. (2022) *'Hacktivist' polarizes Indonesian netizens after data breach spree*, *Asia News Network*. Available at: https://asianews.network/hacktivist-polarizes-indonesian-netizens-after-data-breach-spree/ (Accessed: 19 July 2023).

Joko Widodo | Biography & Facts | Britannica (2023). Available at: https://www.britannica.com/biography/Joko-Widodo (Accessed: 16 June 2023).

Jorion, P. (2010) 'Risk Management', *Annual Review of Financial Economics*, 2, pp. 347–365.

Jurriëns, E. and Tapsell, R. (2017) *DIGITAL INDONESIA CONNECTIVITY AND DIVERGENCE*.

Karacasulu, N. and Uzgören, E. (2007) 'EXPLAINING SOCIAL CONSTRUCTIVIST CONTRIBUTIONS TO SECURITY STUDIES', *PERCEPTIONS: Journal of International Affairs*, 12(3), pp. 27–48.

Kaspersky (2023) *STATISTICS | Kaspersky Cyberthreat real-time map*, *STATISTICS | Kaspersky Cyberthreat real-time map*. Available at: https://cybermap.kaspersky.com/stats (Accessed: 25 June 2023).

Kaspersky (no date) *STATISTICS | Kaspersky Cyberthreat real-time map*, *STATISTICS | Kaspersky Cyberthreat real-time map*. Available at: https://cybermap.kaspersky.com/stats (Accessed: 19 July 2023).

Kaur, D. (2023) *Unpacking cybersecurity in APAC with Fortinet*, *Tech Wire Asia*. Available at: https://techwireasia.com/2023/03/unpacking-cybersecurity-in-apac-with-fortinet/ (Accessed: 19 July 2023).

Kemp, S. (no date a) *Digital 2022: Indonesia*, *DataReportal – Global Digital Insights*. Available at: https://datareportal.com/reports/digital-2022-indonesia (Accessed: 19 November 2022).

Kemp, S. (no date b) *Digital 2022: The Philippines*, *DataReportal – Global Digital Insights*. Available at: https://datareportal.com/reports/digital-2022-philippines (Accessed: 19 November 2022).

Kim, F. (no date) 'Philippines tightening cyber defenses as attacks surge', *Indo-Pacific Defense Forum*. Available at: https://ipdefenseforum.com/2021/12/philippines-tightening-cyber-defenses-as-attacks-surge/ (Accessed: 19 July 2023).

Kroll (2022) *APAC State of incident response 2022*. Available at: https://www.kroll.com/-/media/kroll/pdfs/publications/apac-state-of-incident-response-2022.pdf (Accessed: 13 May 2023).

L., A. (no date) *Stuxnet : zoom sur la « cyber-arme » et comment s'en protéger*. Available at: https://www.cyberuniversity.com/post/stuxnet-zoom-sur-la-cyber-arme-et-comment-sen-proteger (Accessed: 19 July 2023).

Labs, C. (no date) *LuminousMoth - Another Chinese APT Targeting Asian Governments | Cyware Hacker News*, *Cyware Labs*. Available at: https://cyware.com/news/luminousmoth-another-chinese-apt-targeting-asian-governments-9065ccd0 (Accessed: 9 July 2023).

Laqui, C.P. (2022) 'Philippines sees rise in cyberattacks targeting home-based employees' device, says cybersecurity firm', *Interaksyon*, 28 June. Available at: https://interaksyon.philstar.com/trends-spotlights/2022/06/28/220760/philippines-rise-cyberattacks-targeting-home-based-employees-device/ (Accessed: 19 July 2023).

Lechtik, M. (2021) *LuminousMoth APT: Sweeping attacks for the chosen few*. Available at: https://securelist.com/apt-luminousmoth/103332/ (Accessed: 9 July 2023).

LeClair, J., Abraham, S. and Shih, L. (2013) 'An Interdisciplinary Approach to Educating an Effective Cyber Security Workforce', in *Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference*.

New York, NY, USA: Association for Computing Machinery (InfoSecCD '13), pp. 71–78. Available at: https://doi.org/10.1145/2528908.2528923.

Less freedom for Indonesia's internet (2022) *East Asia Forum*. Available at: https://www.eastasiaforum.org/2022/11/12/less-freedom-for-indonesias-internet/ (Accessed: 19 July 2023).

Lin, P.-C. and Liang, C.Y.C. (2019) 'Assessing the Growth Effect of Financial Liberalization in the Presence of Financial Crises: A Case Study of Tiger Cub Economies', *The Developing Economies*, 57(2), pp. 159–193. Available at: https://doi.org/10.1111/deve.12194.

Llewellyn, A. (2022) *Bjorka, the Online Hacker Trying To Take Down the Indonesian Government*. Available at: https://thediplomat.com/2022/09/bjorka-the-online-hacker-trying-to-take-down-the-indonesian-government/ (Accessed: 13 November 2022).

Loviana, K. and Karim, M.P. (no date) 'Cybersecurity and Cyber Resilience in Indonesia':

Manantan, M.B. (2019) 'STRATEGIC INSIGHT 2019 SELECTED COMMENTARIES ON PHILIPPINE FOREIGN RELATIONS AND REGIONAL AFFAIRS : How to Build a Cyber-Resilient Philippines'. Available at: https://appfi.ph/images/2019/Publications/Strategic_Insight_2019_vol_1.pdf#page=53.

Mandiant (2022) *M-Trends-2022-Report.pdf*. Available at: https://mandiant.widen.net/s/bjhnhps2mt/m-trends-2022-report (Accessed: 25 June 2023).

Mandiant (2023) *m-trends-2023.pdf*. Available at: https://mandiant.widen.net/s/dlzgn6w26n/m-trends-2023 (Accessed: 25 June 2023).

Master of Law, Universitas Diponegoro (2022) 'The Effectiveness of Indonesian National Police Strategy in Cybercrime Eradication through ASEAN Ministerial Meeting on Transnational Crime (AMMTC)', *International Journal of Social Science and Human Research*, 05(08). Available at: https://doi.org/10.47191/ijsshr/v5-i8-42.

Matthews, J.R. (2011) 'Assessing Organizational Effectiveness: The Role of Performance Measures', *The Library Quarterly: Information, Community, Policy*, 81(1), pp. 83–110. Available at: https://doi.org/10.1086/657447.

Mcbeth, J. (2022) *Why cyber hackers have such big eyes for Indonesia*, *Asia Times*. Available at: https://asiatimes.com/2022/09/why-cyber-hackers-have-eyes-for-indonesia/ (Accessed: 19 July 2023).

McGettrick, A. (2013) 'Toward Effective Cybersecurity Education', *IEEE Security & Privacy*, 11(6), pp. 66–68. Available at: https://doi.org/10.1109/MSP.2013.155.

MEC Networks Corporation (2022) *The Cybersecurity Threat Landscape in the Philippines 2022 (Infographic)* •. Available at: https://mec.ph/infographics/cybersecurity-threat-landscape-2022/ (Accessed: 13 May 2023).

Mezo (2019) *LuminousMoth APT*. Available at: https://www.enigmasoftware.fr/luminousmothapt-supprimer/ (Accessed: 9 July 2023).

Microsoft defines digital threat landscape, advocates for stronger defense and resiliency in the Philippines – Microsoft News Center Philippines (no date). Available at: https://news.microsoft.com/en-ph/2022/11/25/microsoft-defines-digital-threat-landscape-advocates-for-stronger-defense-and-resiliency-in-the-philippines/ (Accessed: 19 July 2023).

Montibeller, G. and Franco, L.A. (2007) *Decision and risk analysis for the evaluation of strategic options*. Available at: https://www.researchgate.net/profile/L-Franco-

3/publication/41663399_Decision_and_risk_analysis_for_the_evaluation_of_strategic_options/links/55a4d7b308ae81aec91317a1/Decision-and-risk-analysis-for-the-evaluation-of-strategic-options.pdf (Accessed: 28 May 2023).

Mulyadi and Rahayu, D. (2018) 'Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN)', in *2018 6th International Conference on Cyber and IT Service Management (CITSM)*. *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, pp. 1–6. Available at: https://doi.org/10.1109/CITSM.2018.8674265.

Mylrea, M., Gourisetti, S.N.G. and Nicholls, A. (2017) 'An introduction to buildings cybersecurity framework', in *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*. *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1–7. Available at: https://doi.org/10.1109/SSCI.2017.8285228.

Nadua, F. *et al.* (2023) 'Identifying Incentives to Address Attrition in the Government Cybersecurity Workforce'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.4382110.

Nair, P. (no date) *Indonesian Intelligence Agency Reportedly Breached*. Available at: https://www.bankinfosecurity.asia/indonesian-intelligence-agency-reportedly-breached-a-17518 (Accessed: 30 June 2023).

Nardin, T. and Mapel, D.R. (1992) *Traditions of International Ethics*. Cambridge University Press.

National Audit Office (2013) *The UK cybersecurity strategy: Landscape review*. Available at: https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf (Accessed: 12 June 2023).

NCSI (no date a) *NCSI :: Methodology*. Available at: https://ncsi.ega.ee/methodology/ (Accessed: 23 November 2022).

NCSI (no date b) *NCSI :: Ranking*. Available at: https://ncsi.ega.ee/ncsi-index/?order=rank (Accessed: 15 November 2022).

New Stuxnet Malware Most Widespread in Indonesia and Iran (no date). Available at: https://www.spamfighter.com/News-14834-New-Stuxnet-Malware-Most-Widespread-in-Indonesia-and-Iran.htm (Accessed: 19 July 2023).

NIST (2018) 'Cybersecurity Framework Components', *NIST* [Preprint]. Available at: https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components (Accessed: 18 July 2023).

NIST (2023) 'Quick Start Guide', *NIST* [Preprint]. Available at: https://www.nist.gov/cyberframework/getting-started/quick-start-guide (Accessed: 18 July 2023).

NQA (no date) *ISO 27002:2022 – A GUIDE TO THE CHANGES*. Available at: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/NQA-Webinar-A-guide-to-the-changes-to-ISO-27002.pdf (Accessed: 19 July 2023).

Octopus Cybercrime Community (no date) *The Philippines - Status regarding Budapest Convention*, *Octopus Cybercrime Community*. Available at: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/philippines/pop_up (Accessed: 28 March 2023).

'PAGBA History – PAGBA' (2013), 23 March. Available at: https://www.pagba.com/history/ (Accessed: 19 July 2023).

Parameswaran, P. (2015) *Indonesia's Cyber Challenge Under Jokowi*. Available at: https://thediplomat.com/2015/01/indonesias-cyber-challenge-under-jokowi/ (Accessed: 17 June 2023).

Paté-Cornell, M.-E. *et al.* (2018) 'Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies', *Risk Analysis*, 38(2), pp. 226–241. Available at: https://doi.org/10.1111/risa.12844.

Personal data of 105m Indonesian citizens leaked online (2022) *Cybernews*. Available at: https://cybernews.com/news/hackers-leak-sensitive-data-of-over-105m-indonesian-citizens/ (Accessed: 19 July 2023).

Philippines News Agency (2022) *PH 4th among countries most targeted by web threats*. Available at: https://www.pna.gov.ph/articles/1168257 (Accessed: 14 May 2023).

Post, T.J. (no date a) *Hacker breaches data of 34 million Indonesian passports*, *The Jakarta Post*. Available at: https://www.thejakartapost.com/indonesia/2023/07/06/hacker-breaches-data-of-34-million-indonesian-passports.html (Accessed: 19 July 2023).

Post, T.J. (no date b) *Jokowi calls on fintechs to adopt good governance for enhanced cybersecurity, services*, *The Jakarta Post*. Available at: https://www.thejakartapost.com/news/2020/11/15/jokowi-calls-on-fintechs-to-adopt-good-governance-for-enhanced-cybersecurity-services.html (Accessed: 19 July 2023).

President Jokowi Hopes to Launch National Cyber Security Agency (no date) *Jakarta Globe*. Available at: https://jakartaglobe.id/news/president-jokowi-hopes-launch-national-cyber-security-agency (Accessed: 19 July 2023).

PricewaterhouseCoopers (no date) *A comparison of cybersecurity regulations: Indonesia*, *PwC*. Available at: https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations.html (Accessed: 19 July 2023).

Ravi Kumar, S. *et al.* (no date) *Recommendations for effective cyber security execution*. Available at: https://ieeexplore.ieee.org/document/7542327/ (Accessed: 19 July 2023).

Reid, R.A., Koljonen, E.L. and Bruce Buell, J. (1999) 'The Deming Cycle Provides a Framework for Managing Environmentally Responsible Process Improvements', *Quality Engineering*, 12(2), pp. 199–209. Available at: https://doi.org/10.1080/08982119908962577.

ReliefWeb (2009) *2009 Indonesia (West Java) earthquake: CWS emergency appeal 10-05-09 - Indonesia |*. Available at: https://reliefweb.int/report/indonesia/2009-indonesia-west-java-earthquake-cws-emergency-appeal-10-05-09 (Accessed: 16 June 2023).

Rep. Ratcliffe, J. [R-T.-4 (2017) *H.R.1616 - 115th Congress (2017-2018): Strengthening State and Local Cyber Crime Fighting Act of 2017*. Available at: http://www.congress.gov/ (Accessed: 28 March 2023).

Resty Woro, Y. (no date) *Indonesia denies report of Chinese hacking group breaching intelligence agency servers | South China Morning Post*. Available at: https://www.scmp.com/week-asia/politics/article/3148680/indonesia-denies-report-chinese-hacking-group-breaching (Accessed: 30 June 2023).

Reuters (2021) 'Indonesia probe police hack in latest cyber breach', *Reuters*, 19 November. Available at: https://www.reuters.com/world/asia-pacific/indonesia-probe-police-hack-latest-cyber-breach-2021-11-19/ (Accessed: 19 July 2023).

Reveron, D.S. (no date) *Cyberspace_and_National_Securit.pdf*, *Google Docs*. Available at: https://drive.google.com/file/d/1B5TDrPiBHhL30iOvnFvtwuXf4-cO3ENH/view?usp=embed_facebook (Accessed: 19 July 2023).

'Révision de la norme ISO27002:2022' (2022) *smartcockpit*, 1 March. Available at: https://www.smartcockpit.ch/revision-de-la-norme-iso-27002/ (Accessed: 19 July 2023).

Rizal, M. and Yani, Y. (2016) 'Cybersecurity Policy and Its Implementation in Indonesia', *JAS (Journal of ASEAN Studies)*, 4(1), p. 61. Available at: https://doi.org/10.21512/jas.v4i1.967.

Robbins, C. (2017) 'The "3D" National Cyber Security Strategy', *Nexor*, 8 February. Available at: https://www.nexor.com/national-cyber-security-strategy/ (Accessed: 19 July 2023).

Rofii, M.S. (2020) 'Strengthening Digital Ecosystems for Sustainable Development in Indonesia: Anticipating Cyber Threats', *IOP Conference Series: Earth and Environmental Science*, 436(1), p. 012026. Available at: https://doi.org/10.1088/1755-1315/436/1/012026.

Saputra, P.N. *et al.* (no date) 'Addressing Indonesia's Cyber Security through Public- Private Partnership (PPP)'.

Seasia.co (no date) *Southeast Asian Countries Cybersecurity Index (2022)*, *Seasia.co*. Available at: https://seasia.co/2022/09/19/southeast-asian-countries-cybersecurity-index-2022 (Accessed: 19 July 2023).

Segundo J. E., R., Jr. (no date) *Duterte's Rise to Power in the Philippines: Domestic and Regional Implications | Heinrich Böll Foundation | Southeast Asia Regional Office*, *Heinrich-Böll-Stiftung*. Available at: https://th.boell.org/en/2016/09/26/dutertes-rise-power-philippines-domestic-and-regional-implications (Accessed: 12 June 2023).

Setiadi, F. (2012) 'An Overview of the Development Indonesia National Cyber Security', *International Journal of Information Technology & Computer Science*, 6.

Skleparis, D. (2016) '(In)securitization and illiberal practices on the fringe of the EU', *European Security*, 25(1), pp. 92–111. Available at: https://doi.org/10.1080/09662839.2015.1080160.

SocRadar (2021) '2021 Indonesia Threat Landscape Report'.

SocRadar (2023) *SocRadar Threat Landscape in Indonesia 2023*. Available at: https://reports.socradar.com/pdfs/2023-05-07/8ecb5619610743a1b44f85c5703d9b88.pdf (Accessed: 13 May 2023).

SocRadar (no date) *SocRadar Threat Landscape in The Philippines 2022*. Available at: https://reports.socradar.com/pdfs/2023-05-07/c7989747db694853bb8788e39d181821.pdf (Accessed: 19 July 2023).

Sosa, G.C. (no date) 'COUNTRY REPORT ON CYBERCRIME: THE PHILIPPINES'.

Srinivas, J. (2019) 'Government regulations in cyber security: Framework, standards and recommendations', *Future Generation Computer Systems*, 92, pp. 178–188. Available at: https://doi.org/10.1016/j.future.2018.09.063.

Stuxnet: Les origines – Kaspersky Daily – (2014). Available at: https://www.kaspersky.fr/blog/stuxnet-les-origines/3939/ (Accessed: 19 July 2023).

Sunkpho, J., Ramjan, S. and Ottamakorn, C. (no date) 'Cybersecurity Policy in ASEAN Countries'.

Swamidass, P.M. (ed.) (2000) 'Deming cycle (PDCA)DEMING CYCLEPlan-do-check act (PDCA)(PDCA)', in *Encyclopedia of Production and Manufacturing Management*. Boston, MA: Springer US, pp. 155–155. Available at: https://doi.org/10.1007/1-4020-0612-8_229.

Sy, G.L. (2015) *Short History of the Development of Cybercrime*. Available at: https://doj.gov.ph/files/cybercrime_office/Short%20History%20of%20the%20Dvlpt%20of%20Cybercrime.pdf (Accessed: 9 July 2023).

Tan, A. (2023) *New APT group targets ASEAN governments and militaries | Computer Weekly*, *ComputerWeekly.com*. Available at: https://www.computerweekly.com/news/252529069/New-APT-group-targets-ASEAN-governments-and-militaries (Accessed: 13 May 2023).

The Asia Foundation (2022) *Cybersecurity in the Philippines Global Context and Local Challenges*. Available at: https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf (Accessed: 25 April 2023).

The Hacker News (2022) *2022 Top Five Immediate Threats in Geopolitical Context*, *The Hacker News*. Available at:

https://thehackernews.com/2022/12/2022-top-five-immediate-threats-in.html (Accessed: 13 May 2023).

The Jakarta Post (2023) *Hacker breaches data of 34 million Indonesian passports*, *Asia News Network*. Available at: https://asianews.network/hacker-breaches-data-of-34-million-indonesian-passports/ (Accessed: 18 July 2023).

The New York Times (2000) 'Philippine President Signs Law to Punish Computer Crimes', 15 June. Available at: https://www.nytimes.com/2000/06/15/technology/philippine-president-signs-law-to-punish-computer-crimes.html (Accessed: 18 July 2023).

Tianfield, H. (2016) 'Cyber Security Situational Awareness', in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 782–787. Available at: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.165.

Timmerman, A. (2022) *Sick of data leaks, Indonesians are siding with a hacker who exposed 1.3 billion SIM card details*, *Rest of World*. Available at: https://restofworld.org/2022/indonesia-hacked-sim-bjorka/ (Accessed: 12 November 2022).

Translation, O. of A. to D.C.S. for S.D.& (2022) *President Jokowi Issues Presidential Regulation on Protection for Vital Information Infrastructure*, *Sekretariat Kabinet Republik Indonesia*. Available at: https://setkab.go.id/en/president-jokowi-issues-presidential-regulation-on-protection-for-vital-information-infrastructure/ (Accessed: 19 July 2023).

Ulum, M. (2018) *CYBER CULTURE AND CYBER SECURITY POLICY OF INDONESIA: COMBINING CYBER SECURITY CIVIC DISCOURSE, TENETS AND COPENHAGEN'S SECURITIZATION THEORY ANALYSIS*.

US Government (2003) *The National Strategy to Secure Cyberspace*. Available at: https://georgewbush-whitehouse.archives.gov/pcipb/ (Accessed: 12 June 2023).

Vasquez, J.A. (1998) *The Power of Power Politics: From Classical Realism to Neotraditionalism*. Cambridge University Press.

Wahono, T. (2010) *34.000 Komputer di Indonesia Terinfeksi Stuxnet*, *KOMPAS.com*. Available at: https://tekno.kompas.com/read/2010/10/04/23074744/34.000.Komputer.di.Indonesia.Terinfeksi.Stuxnet (Accessed: 25 June 2023).

Walters, R. and Novak, M. (2021) 'The Philippines', in R. Walters and M. Novak (eds) *Cyber Security, Artificial Intelligence, Data Protection & the Law*. Singapore: Springer, pp. 197–220. Available at: https://doi.org/10.1007/978-981-16-1665-5_8.

What Is the Balance of Power and How Is it Maintained? | Walden University (no date). Available at: https://www.waldenu.edu/online-doctoral-programs/phd-in-public-policy-and-administration/resource/what-is-the-balance-of-power-and-how-is-it-maintained (Accessed: 19 July 2023).

Wildavsky, A. and Dake, K. (1990) 'Theories of Risk Perception: Who Fears What and Why?'

Williams, P.D. and McDonald, M. (2018) *Security Studies : An Introduction*. Available at: https://ebookcentral.proquest.com/lib/gla/detail.action?docID=5295090 (Accessed: 9 June 2023).

Winger, G.H. (2022) 'Cybersecurity in the U.S.-Philippine alliance: mission seep', *The Pacific Review*, pp. 1–29. Available at: https://doi.org/10.1080/09512748.2022.2112064.

Yasar, K. (no date) *What is a RAT (Remote Access Trojan)? | Definition from TechTarget*. Available at:

https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan (Accessed: 30 June 2023).

Zero-Day Vulnerability - Definition (no date). Available at: https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability (Accessed: 26 June 2023).

II. Annexe

Annex 1: Filipino Cyber Security Framework