Journal of Social Political Sciences
JSPS
Vol. 2, No. 4, Nov, 2021

SYNERGY OF MULTI-STAKEHOLDERS IN DEFENDING INDONESIA FROM CYBER THREATS

Aththaariq Rizki[1], Fauzia Gustarina Cempaka Timur[2]
1Student of Asymmetric Warfare Study Program, Indonesia Defense University, Bogor
2Lecturer in Asymmetric Warfare Study Program, Indonesia Defense University, Bogor
Email: erikatorik@gmail.com, fg.cempaka@idu.ac.id

Abstract: This paper argues that currently the threat of cyber-attacks has become a real threat that has the potential to develop in Indonesia. With the presence of these cyber-attacks, the government must take advantage of the synergy between state multi-stake holders to jointly face cyber threats that come to attack Indonesia. The purpose of this research is to answer the existing problem formulations, namely first to find out which state multi-stake holders are in synergy in defending cyber-attacks in Indonesia; and to analyze how the synergy of state multi-stake holders in dealing with cyber-attacks in Indonesia. The writing of this article was conducted using a qualitative method with a literature review approach that focuses on the synergy between state multi-stake holders in dealing with cyber-attacks in Indonesia. The theory used is the concept of synergy, state multi-stake holders, and the threat of cyber-attacks as a literature review. In this paper, the results show that the synergy concept consists of coordination; and communication, which is used by state multi-stake holders to face the threat of cyber-attacks. So that it can be concluded from this writing that state multi-stake holders who work together in defending cyber threats are: BSSN, Kominfo, Puskom Kemhan, Pusinfolahta TNI Headquarters, and Dittipidsiber Polri. In addition, the synergy of state multi-stake holders in dealing with cyber-attacks in Indonesia is carried out by applying the synergy aspect, namely coordination and communication, which is led by BSSN as the leading sector in the cyber defense sector.

Keyword: Synergy, Stakeholder, Cyber, Attack, Indonesia.

Submission	:	Aug 7th 2021
Revision	:	Sept 18th 2021
Publication	:	Nov 28th 2021

INTRODUCTION

The development of technology in the world is currently growing very rapidly. Starting from daily activities to professional activities utilizing technology in their activities. But in addition to providing benefits, technological developments can also have a negative impact on humans. One of the technology-based threats that is currently being carried out is cyber threats. Cyber threats are a new challenge and problem that must be faced by the government. One of the major cyber-attack cases that the Indonesian people have ever faced is the WannaCry ransomware cyber-attack. In 2018, the world was shocked by the WannaCry cyber-attack, no more than 150 countries were affected by this cyber-attack. Indonesia was also one of the victims of this attack,

one of the institutions that was attacked was the hospital. According to Kertopati in CNN Indonesia (2018), the Ministry of Communication and Information of the Republic of Indonesia (Kominfo) said that two hospitals in Jakarta were victims of the WannaCry ransomware cyber-attack. These two hospitals are Harapan Kita Hospital and Dharmais Hospital.

Malware attacks the victim's computer by locking the computer or encrypting all existing data so that it cannot be accessed again. To unlock and re-access the computer, the victim must pay a ransom to the sender of the virus. This is a big problem, considering the hospital is a critical infrastructure in a country. If the existing system in the hospital is paralyzed, the health services provided will also be hampered. The National Cybersecurity Operations Center (Pusopskamsinas) of the National Cyber and Crypto Agency (BSSN) noted that there were 88,414,296 cyberattacks that occurred from January 1 to April 12, 2020. When the Work from Home (WFH) policy was enacted, many cyber-attacks continued. attack. In January and February 2020, there was a cyber-attack using the background of the Covid-19 pandemic, the attack was Malicious Email Phishing. Meanwhile, in March there were 22 cyber-attacks using the background of the Covid-19 pandemic issue. (BSSN, 2021)

According to BSSN (2021), the work from home mechanism can increase the potential risk of cyber attacks, because work that should be done conventionally must be turned into activities through a network. BSSN noted that the Covid-19 pandemic must be addressed by organizations as a momentum to fix information security policies to anticipate cyber incidents. In addition to attacking critical infrastructure, cyber attacks also cause significant losses. Based on data made by Norton Symantec (2016), it was noted that during 2015 to February 2016. The results show that online crime in Indonesia caused a total loss of Rp. 194.6 billion. This condition should be anticipated and minimized the resulting impact. The government as a policy maker must be able to provide sovereignty and security for cyber systems in Indonesia, especially in critical infrastructure. The government actually already has rules regarding cyber crimes starting in 2008, through Law No. 11 of 2008 regarding information and electronic transactions. However, this rule still has many loopholes that have not regulated crimes in the cyber world. Cyber threats will always develop in accordance with technological developments.

Seeing this, the government in 2014 through the Ministry of Defense has made cyber defense guidelines which are listed in the regulation of the minister of defense of the Republic of Indonesia Number 82 of 2014. The guidelines indicate that the government is aware of the dangers of potential cyber attacks. Based on this regulation, it is also explained that in realizing National Cyber Security, every effort is needed from the institution. So that synergy between state multi-stake holders is very important in dealing with cyber attacks that have a broad spectrum of battlefields. The government through Presidential Regulation Number 53 of 2017 concerning the National Cyber and Crypto Agency (BSSN) and its amendment regulations Presidential Regulation Number 133 of 2017 established a BSSN which is tasked with

implementing cyber security effectively and efficiently by utilizing, developing and participating in consolidating all elements related to security. national cyber. (BSSN, 2021)

BSSN in carrying out its duties does not move alone. How many agencies are intersecting each other in carrying out their obligations. The collaboration and integration of these agencies will create a national cyber defense. With the existence of a national cyber defense, the government hopes that cyber attacks that threaten national security can be minimized and prevented as well as possible. The government is aware that if cyber security is left weak, many parties are ready to make Indonesia the target of cyber attacks. One of the toughest challenges is the breadth and massiveness of internet and gadget users in Indonesia. This is one of the challenges that must be faced by state multi-stake holders in dealing with cyber attacks in Indonesia. (BSSN, 2021)

According to Firmansyah (2016) Synergy can be interpreted as an activity to carry out joint operations. Synergy or synergy is the same thing, the term synergy is defined as the activities of groups or individuals from different backgrounds to adjust performance in order to achieve goals. Hampden-Turner in Firmansyah states that synergy activities are actions that involve all activities, these activities will go hand in hand together so as to create something new. Furthermore, Hampden-Turner in Firmansyah (2016) asserts that synergy is the result of a dialogic relationship between different sources of knowledge, and is a process that accumulates various kinds of knowledge. Meanwhile, Najiyati (2011) explains that synergy can be formed through two aspects, namely:

1. Coordination, in this coordination it is necessary to determine the relationship between the relevant stakeholders, whether it is determining the relationship vertically, horizontally, command relationship, or partnership relationship.
2. Communication, in the aspect of communication, there is a process of exchanging information between two or more parties, as well as individuals with other individuals, with the aim that the intended target can understand the information that has been given.

On the other hand, according to Bryson (2005), stakeholders can be interpreted as "any person, group, or organization that pays attention to and makes claims on resources, or organizational results, or what is affected by those results. Freeman and McVea (2001) also define a stakeholder as any individual or group who can influence or be influenced by the achievement of organizational goals. So it can be concluded that a stakeholder is a person or group who pays attention to and claims to resources, or organizational results, which can influence or be influenced by the achievement of organizational goals. In this research, the author chooses state multi-stake holders as the discussion. A state multi-stake holder is a person or group who pays attention to and claims on resources, or organizational results, which can influence or be influenced by the achievement of organizational goals, originating from government or state institutions.

According to Strickling (2017), there is currently no single conceptualization of what is meant by a 'multi-stakeholder approach'. Instead, there are many models currently in use, each with its own unique contours. Only a few models are currently in use, one of which is not always static; rather, they are constantly evolving to meet new and uncharted governance challenges. In this paper, we have tried to use the 'multi-stakeholder model', to see the synergies carried out by state multi-stake holders in dealing with cyber threats in Indonesia. The term 'multi-stakeholder' is often misunderstood and misunderstood, it has become a bit of a buzzword in government circles. Actors often mistakenly and sometimes manipulatively attach the label 'multi-stakeholder' to what is in practice a top-down, multilateral process. It is appropriate, therefore, to outline a definition that serves to reinforce the core values of the internet and to protect the term 'multi-stakeholder' from becoming more of a marketing meme for governance schemes. For that, I use the concept from Strickling (2017), regarding the 'genuine' multi-stakeholder process, namely:

1. Stakeholder driven: Stakeholders define processes and decisions, from agenda setting to workflow, rather than simply fulfilling an advisory role;
2. Open: Every stakeholder can participate and the process includes and integrates the perspectives of multiple stakeholders, the most important of which is the perspective of stakeholders who have specific expertise that can be applied to the governance challenges faced;
3. Transparent: All stakeholders and the public have access to deliberation, creating an environment of trust, legitimacy and accountability;
4. Consensus-based: Outcomes (when outcomes are desired) are based on consensus, reached by compromise, and are a win-win for the greatest number or diversity of stakeholders.

From the background review above, two problem formulations are obtained, namely the state multi-stake holders who are synergizing in dealing with attacks in Indonesia and know about the synergy between state multi-stake holders in dealing with cyber attacks in Indonesia. Based on the formulation of the problem above, the purpose of this study is to find out which state multi-stake holders are synergizing in dealing with cyber attacks in Indonesia. As well as to analyze how the synergy of state multi-stake holders in dealing with cyber attacks in Indonesia.

METHOD

Our study focuses on how the synergy between multi-stakeholders can be a force to defend Indonesia from cyber threats by maximizing the use of information and communication technology. In writing this scientific paper, the author uses a qualitative research method with a literature review approach. According to Creswell (2013), literature review is a research approach that is based on non-numeric data, which can be in the form of text and images, and filtered data to interpret the literature review. With this research method, the author can obtain

data collection through library sources such as journals, books, theses, research reports, and scientific articles with valid and reliable sources. In this case, the data obtained includes data released by the Indonesian government on web pages and reports, newspapers, journals, books, websites, and other published materials that have certain credibility.

RESULT

Stakeholders of the State Organizing the National Cyber Security System in Indonesia

According to Siagian et al (2018), the stake holders of the national cyber security system organizers in Indonesia are composed of four government agencies, namely BSSN, KOMINFO, Puskom KEMHAN, and Pusinfolahta TNI Headquarters. Meanwhile, according to Subagyo (2015) adding the POLRI cyber agency as one of the organizers of the national security system. Therefore, there are six state institutions that have a role in running the national cyber security system.

1. National Cyber and Crypto Agency (BSSN)

   BSSN is one of the non-ministerial government agencies whose main objective is to implement cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to national cyber security. Based on the profile information on the BSSN website (2021), BSSN has the authority to formulate the Indonesian Cyber Security Strategy as a joint reference for all national cyber security stakeholders in order to formulate and develop cyber security policies in their respective agencies. In the preparation of cyber strategies, BSSN must still be guided by the basic values of national and state life, namely: sovereignty, security, independence, adaptability, and also the value of togetherness.

2. Ministry of Communication and Informatics RI

   Quoted from the official website of the Ministry of Communication and Information (2021), according to Law Number 39 of 2008 concerning State Ministries, the Ministry of Communications and Informatics is an agency and apparatus of the Government of the Republic of Indonesia that is in charge of affairs with the scope area as stated in the Constitution of the Republic of Indonesia Year 1945, namely information and communication. The Ministry of Communication and Information Technology has the main task of carrying out government affairs in the field of communication and information technology in order to assist the President in administering the state government. The Ministry of Communication and Informatics is led by a Minister of Communication and Information (Menkominfo).

3. The Indonesian Ministry of Defense Center

   Based on the official page of Puskom Kemhan (2021), Puskom Kemhan is one of the state institutions with a supporting function in the ministry of defense in the field of communication and information. Based on the Regulation of the Minister of Defense of the

Republic of Indonesia Number 58 of 2014 the Indonesian Ministry of Defense Puskom or the Center for Public Communication is a supporting element for implementing defense tasks and functions under and responsible to the Minister.

4. Pusinfolahta TNI Headquarters

   Based on the history of Pusinfolahta quoted from the Pusinfolahta website (2021), it is explained that the TNI Information and Data Processing Center (Pusinfolahta TNI) was established based on the Decree of the TNI Commander Number Kep/7/XII/2006 dated December 5, 2006 as the Central Implementing Body at the TNI Headquarters level. which is located directly under the TNI Commander with the main task of preparing information and data processing for the guidance and use of TNI forces, carrying out the function of developing TNI information systems for Leaders and Staff within the TNI Headquarters as well as developing computer systems and data communication in the context of carrying out the TNI's main tasks.

5. Dittipidsiber Polri

   Based on information through the official page of Dittipidsiber (2021), it was found that the Directorate of Cyber Crime (Dittipidsiber) is a work unit under the Criminal Investigation Unit of the National Police and is tasked with enforcing the law against cybercrimes. In general, Dittipidsiber handles two groups of crimes, namely computer crime and computer-related crime. Computer crime is a group of cybercrimes that use computers as the main tool. The forms of crime are hacking of electronic systems, illegal interception, changing the appearance of websites (web defacement), system interference, and data manipulation. Computer-related crime is a cybercrime that uses a computer as a tool, such as online pornography, online gambling, online defamation, online extortion, and online fraud. network (online fraud), hate speech, threats in the network (online threat), illegal access, and data theft.

6. LIPI

   LIPI is the first, largest and best research institute in Indonesia. The establishment of LIPI has a long history. After going through several phases of scientific activity from the 16th century to 1956, the Indonesian government established the Indonesian Science Council (MIPI) through Law (UU) No. 6 of 1956. Its task is to guide the development of science and technology as well as give consideration to government in terms of scientific policy. LIPI has a vision to become a world-class scientific institution in research, development and utilization of science to improve the nation's competitiveness. LIPI itself is a representative body as an academic party in helping cyber defense. (LIPI, 2021)

DISCUSSION

Synergy of State multi-stake holders in Defending Cyber Attacks in Indonesia.

Currently, every cybersecurity provider has their own duties and roles. Even though they have different duties and responsibilities, each organizer must also be able to work together, synergize, and help each other. In order to realize good synergy in dealing with cyber-attacks. There needs to be a common view and purpose. At this time, since 2017, through Presidential Regulation of the Republic of Indonesia No. 53 of 2017 BSSN has the task of implementing cyber security effectively and efficiently by utilizing, developing, and consolidating all elements related to cyber security.

So, it can be analyzed that at this time BSSN is the institution that regulates all the synergies and elements that exist in cyber security. If the level of cyber handling is made, then currently BSSN is in charge of each other organizer. In order to support the cyber doctrine and BSSN, the TNI Doctrine "Tri Dharma Eka Karma" also includes the cyber security doctrine under it. Where at this time all parties must help each other in maintaining cyber security. In order to safeguard the country's security from cyber attacks, the Government of Indonesia can apply the Strickling (2017) concept of a 'genuine' multi-stakeholder process. That way, the synergies that will be built later by state multi-stake holders will be able to better handle cyber threats. As for the things that must be done by the Government of Indonesia related to the Strickling multi-stakeholder concept, among others:

1. Stakeholder driven: Indonesian stakeholders must be able to define processes and decisions to deal with existing cyber threats, from agenda setting to workflow, rather than simply fulfilling an advisory role. Currently, Indonesian stakeholders have been able to make decisions to deal with cyber threats, one example of which is the establishment of the Cyber Defense Manual in 2014.
2. Open: Every stakeholder of the Government of Indonesia must be able to participate and integrate the perspectives of various other stakeholders, the most important of which is the perspective of stakeholders who have special expertise that can be applied to the governance challenges faced. For example, BSSN as a leading sector in the field of cyber defense must be able to be open and accept the perspectives of other stakeholders in dealing with cyber threats. So that the handling of cyber threats is not seen from one side only.
3. Transparent: All GoI stakeholders and the public have access to deliberation, creating an environment of trust, legitimacy and accountability. The Indonesian government must create a transparent government system to increase public trust. Deliberations for consensus in dealing with cyber threats need to be used to receive input from various points of view. A trusted environment and clear legitimacy can also increase the effectiveness of handling existing cyber threats. This has been done by giving legitimacy to the BSSN which has been legally appointed to become the leading sector in the field of cyber defense.
4. Consensus-based: The Government of Indonesia should be able to determine outcomes that are based on consensus, reached by compromise, and are win-win for the greatest number

or diversity of stakeholders. So that to determine the results of the policies that will be developed later, the Government of Indonesia through the BSSN must be able to reach compromises and agreements with other stakeholders to be able to make a result and decision.

According to the Head of BSSN Djoko Setiadi in BSSN (2021), it is explained that there are several steps that need to be taken so that it is expected to be able to prevent and minimize the impact of every cyber threat and attack. In this case, collaboration, coordination, and synergy efforts, as well as information sharing are the right steps. One form of collaboration, coordination, synergy, and information sharing is through the relationship between BSSN as an institution that handles the field of Indonesian cyber security, with stakeholders. In terms of collaboration, one of the things that BSSN does is collaborate with LIPI to form a Cyber Incident Response Team or Computer Security Incident Response Team (CSIRT). The establishment of the CSIRT has been in line with the implementation of the Electronic-Based Government System (SPBE). In Presidential Regulation Number 95 of 2018 concerning SPBE it is stated that as an element of SPBE security, namely guaranteeing the integrity and availability of data and information. (BSSN, 2021).

In terms of coordination, reported by Kominfo (2017), Coordinating Minister for Political, Legal and Security Affairs Wiranto said that based on the results of the meeting, BSSN would be directly under the command of the Ministry of Political, Legal and Security Affairs, not under the coordination of President Joko Widodo. So that in order to coordinate upwards, BSSN will coordinate directly with the Kemenpolhukam to carry out its activities. In terms of synergy, BSSN also carries out synergistic activities for several other stakeholders. One of the things to do is to synergize with Kominfo. Reported from Kominfo (2021), the Ministry of Communication and Information together with the National Cyber and Crypto Agency (BSSN) formed the Kominfo-Computer Security Incident Response Team (CSIRT). Secretary General of the Ministry of Communication and Informatics Mirra Tayyiba stated, KCSIRT is intended to anticipate cyber security incidents within the Ministry of Communication and Information. KCSIRT has three main objectives, including realizing reliable and professional cyber resilience, coordinating and collaborating cyber security services, and building cyber security resource capacity. In addition, to conduct information sharing, BSSN carries out several activities to share information with other stakeholders and the public. One of the activities carried out was organizing Community Building and Information Sharing which was attended by High Officials from the BSSN, Bais TNI, Criminal Investigation Police, Bainstranas Kemhan, BIN, and the cyber security community. (BSSN, 2019)

In accordance with Subagyo's opinion (2015), cyber-attacks can be divided and escalated into: cyber threats, cybercrimes, and cyber wars. If the division of stakeholder tasks is divided into the cyber-attack escalation table, the organizers will be divided into:

Tabel 1. Cyber Attack Escalation

No	Threat Type	Stakeholder
1	Cyber Threat	Kemhan, Kominfo, BSSN, LIPI
2	Cyber Crime	Dittipidsiber Polri, BSSN, LIPI
3	Cyber War	Kemhan, TNI, BSSN

Source: Research Results, 2021

In table 1, it can be seen that the BSSN plays a role in every escalation of existing threats, because the task of the BSSN is to maintain the overall cyber security in Indonesia. Each organizer can also intersect with each other in terms of handling a case. The wide spectrum of the cyber world requires every organizer to always work together. This is where the role of BSSN which should also be able to be every liaison and monitor how cyber security is running in Indonesia. Based on the synergy theory, Najiyati (2011) explains that synergy can be formed through two aspects, namely coordination and communication. Therefore, BSSN in synergizing with stakeholders from other countries needs to focus on coordination and communication. The steps that must be taken by BSSN to maintain Indonesian cyber security in accordance with the synergy theory include:

1. BSSN in terms of making policies that function to fend off, counteract, and prevent cyber threats that can harm communication networks, government agencies, and private institutions related to communication and informatics must establish coordination and communication with Kominfo as related institutions in the formation of policies in the field of ICT.
2. Regarding the threat of cyber warfare, BSSN must coordinate and communicate with the Indonesian National Armed Forces Headquarters Pusinfolahta institution regarding the processing of information on TNI resilience in order to maintain national cyber security. In the event of a cyber war, BSSN, Pusinfolahta TNI Headquarters, and Puskom Kemhan are the foremost organizers who carry out defense and resistance. It is very important to

coordinate and communicate together regarding war strategies and plans that will be used in cyber warfare.

3. As for dealing with cybercrimes. BSSN can coordinate and communicate with the Dittipidsiber Polri related to crime tracking, cybercrime handling, cybercrime anticipation, and cyber-crime prevention. The National Police can also ask for assistance from the BSSN in the context of asset security operations, or seeking information on suspected cybercriminals.
4. The BSSN must also coordinate communication with the Ministry of Defense Communications Center regarding Indonesia's cyber defense situation in terms of cyber warfare, both with domestic and foreign parties. BSSN together with the Ministry of Defense must develop a cyber defense strategy that can be used to protect Indonesia's cyber space, in the context of realizing national security in the cyber field.

CONCLUSION

Currently the threat is no longer limited to physical and military threats. Cyber-attacks are considered a real threat that can happen at any time, and attack anyone. Cyber-attacks also have a fairly broad and dynamic spectrum, so special handling strategies are needed to deal with them. For this reason, currently there are six state multi-stake holders who act as organizers of the National Cyber Security System in Indonesia, including BSSN, Kominfo, Puskom Kemhan, Pusinfolahta TNI Headquarters, LIPI and Dittipidsiber Polri. Currently, cyber-attacks can escalate into cyber threats, cybercrimes, and cyber wars. Each of these attack areas is ready to be handled by the cybersecurity provider according to its capacity. Cyber threats will be handled by the Puskom Kemhan, Kominfo, and BSSN. Cybercrimes will be handled by the National Police's Dittipidsiber, BSSN. Meanwhile, cyber warfare will be handled by the Communication Center of the Ministry of Defense, Pusinfolahta TNI Headquarters, BSSN. In terms of cyber defense, BSSN here plays the role of Sector Leader and cyber doctrine in Indonesia, so that BSSN has an important role in building a strong cyber defense for Indonesia.

The steps that must be taken by BSSN to maintain Indonesian cybersecurity in accordance with the synergy theory include: (1) Coordinate and communicate with Kominfo in making policies related to ICT; (2) Coordinate and communicate with the Puskom Kemhan and Pusinfolahta TNI Headquarters in the event of cyber warfare; (3) Coordinate and communicate with the National Police's Dittipidsiber regarding the handling of cybercrimes; and (4) Coordinate and communicate with the Ministry of Defense and the Ministry of Defense Communications Center regarding the development of a cyber defense strategy in Indonesia. Seeing the number of cyber attacks that have occurred in Indonesia, it is important for the government to take appropriate measures to deal with cyber threats. The steps

mentioned above are important for the Indonesian government to establish necessary efforts to defend Indonesia from the threat of cyber attacks.

REFERENCES

Ardiyanti, Handrini. (2014). "Cyber-Security dan Tantangan Pengembangannya di Indonesia". Jurnal Politica Vol. 5 No. 1 Juni 2014.

Bryson, John M. (2005). "Perencanaan Strategis Bagi Organisasi Sosial". Yogyakarta: Pustaka Pelajar.

BSSN. (2021). "Kolaborasi BSSN dan LIPI Luncurkan Tim Tanggap Insiden Siber LIPI-CSIRT Ciptakan Ruang Siber yang Aman dan Kondusif". Jakarta: BSSN. In https://bssn.go.id/kolaborasi-bssn-dan-lipi-luncurkan-tim-tanggap-insiden-siber-lipi-csirt-ciptakan-ruang-siber-yang-aman-dan-kondusif/, retrieve at 27 – 09 – 2021.

BSSN. (2021). "Tugas dan Fungsi BSSN". Jakarta: BSSN. In https://bssn.go.id/tugas-dan-fungsi-bssn/, retrieve at 17 – 02 - 2021.

BSSN. (2019). "BSSN Selenggarakan Community Building and Information Sharing Sektor Ekonomi Digital". Jakarta: 2019. In https://bssn.go.id/bssn-selenggarakan-community-building-and-information-sharing-sektor-ekonomi-digital/, retrieve at 27 – 09 – 2021.

Creswell, J. W. (2016). "Research Design Qualitative, Quantitative, and Mixed Methods Approaches" (2nd ed.). Thousand Oaks, California: Sage Publishing.

Firmansyah, M Irwanda. (2016). "Studi Deskriptif Tentang Sinergitas Kewenangan Antara Bpjs Kesehatan dengan Organisasi Profesi dalam Penyediaan Layanan Kesehatan di Kota Surabaya". Journal of Airlangga University Vol 4 No 2 (146 – 156).

Fischer, E. A. (2009). "Creating a National Framework for Cybersecurity: An Analysis of Issues and Options". New York: Nova Science Publishers, Inc.

Freeman, R.E. dan J. McVea. (2001). "A Stakeholder Approach to Strategic". Journal of SSRN. Amerika: Virginia University.

Kementerian Pertahanan Indonesia. (2014). Pedoman Pertahanan Siber. Jakarta: Kemhan RI.

Kementerian Pertahanan Indonesia. (2021). "Rohumas", in https://www.kemhan.go.id/rohumas/category/berita/page/2, retrieve at 17 – 02 – 2021.

Keputusan Panglima TNI Nomor Kep/7/XII/2006 tanggal 5 Desember 2006.

Kertopati, Lesthia. (2018). "Dua Rumah Sakit di Jakarta Kena Serangan Ransomware WannaCry". Jakarta: CNN Indonesia. In https://www.cnnindonesia.com/teknogi/20170513191519192214642/dua-rumah-sakit-di jakarta kena-serangan-ransomware-wannacry, retrieve at 17 – 02 – 2021.

Kominfo. (2021). "Profil", in https://www.kominfo.go.id/profil, retrieve at 17 – 02 – 2021.

Kominfo. (2017). Badan Siber dan Sandi Negara di Bawah Komando Kemenko Polhukam. Jakarta: Kominfo. in https://kominfo.go.id/content/detail/10818/badan-siber-dan-sandi-negara-di-bawah-komando-kemenko-polhukam/0/sorotan_media, retrieve at 27 – 09 – 2021.

Kominfo. (2021). "Kominfo Gandeng BSSN Antisipasi Insiden Keamanan Siber. Jakarta: Kominfo". In https://www.kominfo.go.id/content/detail/35415/siaran-pers-no232hmkominfo072021-tentang-kominfo-gandeng-bssn-antisipasi-insiden-keamanan-siber/0/siaran_pers , retrieve at 27 – 09 – 2021.

Labib, Mohammad dan Wahid, Abdul. (2005). "Kejahatan Mayantara (Cyber Crime)". Bandung: PT. Refika Aditama.

Lauder Siagian, Arief Budiarto, dan Simatupang. (2018). "Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional". Jurnal Prodi Perang Asimetris | Desember 2018, Volume 4, Nomor 3.

Najiyati, Sri dan S.R. Topo Susilo. (2011). "Sinergitas Instansi Pemerintah Dalam Pembangunan Kota Terpadu Mandiri" (The Synergy of Goverment Institutions in The Transmigration Urban Development). Jurnal Ketransmigrasian. Jakarta: Puslitbangtrans.

Nawawi Arief, Barda. (2007). "Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan". Jakarta: Kencana Predana Media Group.

Oona A. Hathaway, et all. (2012). "The Law of Cyber Attack". Journal California Law Review.

Patrolisiber. (2021). "About", in https://patrolisiber.id/about, retrieve at 17 – 02 – 2021.

Peraturan Menteri Pertahanan Republik Indonesia Nomor 58 Tahun 2014.

Peraturan Presiden Republik Indonesia No 53 Tahun 2017.

Pusinfolahtatni. (2021). "Profil", in http://pusinfolahtatni.mil.id/, retrieve at 17 – 02 – 2021.

Sa'diyah, Nur Khalimatus dan Ria Tri Vinata. (2016). "Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara". Jurnal Perspektif Volume XXI No. 3 Tahun 2016 Edisi September.

Strickling, Lawrence E. & Jonah Force Hill. (2017). Multi-stakeholder internet governance: successes and opportunities, Journal of Cyber Policy, 2:3, 296-317, DOI: 10.1080/23738871.2017.1404619

Subagyo, Agus. (2015). "Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy in Defending of Cyber Warfare Threat". Jurnal Pertahanan April 2015, Volume 5, Nomor 1.

Symantec, N. (2016). "Norton Cyber Security Insights Report Global Corporation". Symantec Corp.

Tampubolon, Kartini Eliva Angel. (2019). "Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare". Jurnal Universitas Airlangga.

Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara.