Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

Securitization of Cyber Threats to the Indonesian Government: A Study of Cyber Defense Strategy

Sarwo Edi Wibowo*[1], Ari Hartono[2], Hendri Kiswanto[3], Henike Primawanti[4], Jafirman Torang Avery Louerens[5]
[1,2,3,5]Army Staff and Command School, Indonesia
Jl. Gatot Subroto No. 96, Bandung, Indonesia
[4]International Relations Study Program, Universitas Komputer Indonesia
Jl. Dipati Ukur No. 112-116, Bandung, Indonesia

e-mail: *[1]**sarwoediwibowo141@gmail.com**, [2]ariegi75@gmail.com, [3]hendribumen@gmail.com, [4]henike@email.unikom.ac.id, [5]jafirmantorang@gmail.com

Abstract

The research aims to analyze the cyber threats faced by Indonesia and the issues in them. To achieve this goal, this research explores the Indonesian government's view of cyber security as a non-traditional security threat and the Indonesian government's approach to dealing with cyber threats. It examines the extent to which securitization is carried out by various actors representing the Indonesian government. This research uses a qualitative method with an analytical descriptive form that utilizes direct and indirect sources such as interviews with several informants, literature studies, and documentation studies. This research used a non-traditional security approach, including the securitization theory related to cybersecurity. The finding of this paper suggests that The Ministry of Defense of Indonesia as a state institution did securitization that focuses on the idea of military involvement in securing cyberspace by increasing the current level of cyber technology has been accompanied by an increase in the vulnerability of cybercrime and cyber-attacks both in quality and quantity. The Ministry of Defense formed COC (Cyber Operation Center) as the frontline. It formed the cyber army to strengthen the defense and attack the cyber threat in the Ministry of Defense's area.

Keywords — *Cyber Security, Cyber Threats, Defense Strategy, Ministry of Defense, Securitization.*

1. Introduction

1.1. Background

The phenomenon of cyber space illustrates the reality that the activities of modern society are now interconnected through cyberspace and the internet (Caballero-Anthony, 2016). It is becoming the boon and the bane for a country's security in particular and the whole country and its organ generally. The existence of cyberspace helps the government to ease it administrative tasks and improve the effiecientcy of its governance. Yet, from the perspective of a cyber defense perspective, the use of the internet is also possible for negative or destructive purposes by capable parties. The facilities available on the internet can be used to disrupt, derange, and paralyze a country's crisis infrastructure (Gultom, 2019). Currently, warfare is no longer physical or armed forces, but has shifted to cyber warfare or by computers and internet networks as weapons. In International Relations, this shift is better known as a shift in the concept of traditional security which is militaristic to non-traditional security which is not militaristic in nature (Robert, 2008). Thus, the threats that arise against a country in cyberspace are also very diverse, including, wiretapping in conversations of decision

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

makers in a country, espioniging of state assets through cyberspace, destruction of economic and banking systems, piracy of state websites officials, and attacks on state supporting infrastructure (Kello, 2013).

Roztocki (2019) said that the development of information technology provides significant changes in the concept of security. Now the interaction space not only limited to physical, but also, has extended to the virtual world (cyber) (Roztocki, Soja & Weistroffer, 2019). This has created a new threat pattern that must be faced by the state, namely cyber threats. Cyber threats and attacks can be carried out by actors representing the government (State Actors) or non-government (Non State Actors), so that the perpetrators can be individuals, groups, mass, organizations, or even a country (Buzan & Hansen, 2009; Triwahyuni & Wulandari, 2016).

The most frequent hacking action by various actors in the cyber space is by Denial of Service (DDoS) method. A denial of service (DoS attack) attack is a cyberattack in which the perpetrator attempts to make a machine or network resource unavailable to the intended user by temporarily or indefinitely interrupting the service of an Internet-connected host. Denial of service is usually done by flooding targeted machines or resources with excessive requests in an effort to overload the system and prevent some or all legitimate requests from being met. In distributed denial-of-service attacks, incoming traffic flooding the victims comes from a variety of sources. This effectively makes it impossible to stop an attack by simply blocking one source (Nugraha, 2019).

Indonesia is one of the countries that cannot escape itself from the cyber attacks. It is proven that Indonesia has experienced several cyber attacks which had very detrimental impacts for the government, among them are: Symantec as a producer of Antivirus Norton, announced that Indonesia was in second place after Iran was among the 10 countries that experienced the Stuxnet worm attack in 2010; the WannaCry Ransomware cyber attack in May 2017 that caused disruption to companies and hospitals in more than 150 countries including Indonesia (Sa'diyah, 2017). In addition, one of the official websites of the work unit of the Ministry of Defense of the Republic of Indonesia (Kemhan RI) was attacked by hackers, namely the website of the Directorate General of Defense Potential (Ditjen Pothan) which experienced a page change called defacing. The Directorate General of Defense Potential site was attacked by CVT (Cyber Vampire Team) (Rahmawati, 2017). The attack on the official website of the Defense Potential Directorate General, Ministry of Defense, which was on the www.pothan.kemhan.go.id page was hijacked by hackers from Myanmar. The site's background turned black and was covered with the words:

> *"Oops Myanmar Hacker Was Here'. The writing seems to insinuate the defense of the website of the Indonesian Government. At the bottom there is a long writing in English that reads: "Hello Indonesia Government, You should be proud with uneducated Indo script kiddies. Coz they believe (defacing / Ddosing) to the other country websites is the best solution for them. If you would sympathize the white programmers / developers of your country & how they are feeling. you can catch such script kiddies. coz CVT are ready to provide those skiddies Informations,*" wrote the hacker on the site www.pothan.kemhan.go.id (Rahmawati, 2017).

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

As we can see the magnitude of the cyber threat, the Ministry of Defense of the Republic of Indonesia needs to discuss the strategy and implementation to overcome the threat of cyber attacks by carrying out a securitization process. Securitization is an intersubjective process in the formation of threat perceptions so that it requires fast handling. In its implementation, the Ministry of Defense needs units such as securitizing actors, functional actors and speech acts in shaping threat perceptions so that they are accepted by audiences (Buzan et.al., 1998).

Indonesia as a sovereign country needs to immediately build a cyber defense system to protect the nation's sovereignty and avoid cyber attacks originating from abroad. Currently, the Ministry of Defense of the Republic of Indonesia is making efforts to build a national defense system in the field of cyberspace. In building a defense system, Indonesia already has a framework in the form of the State Defense Doctrine provides the guidance and advice in taking the direction of state policy in the defense sector. National defense doctrine is the basic principles that provides direction for the management of defense resources to achieve national security goals (Widjadjanto, 2005; Soewardi, 2013). This shows that Indonesian Defense Administrators has realized that cyber threats are a real threat for Indonesia, which requires an immediate and a concrete action from the part of Indonesian National Defense Administrators. Therefore, the attempts toward the development of defense forces in order to maintain the sovereignty of Indonesia needs to be directed towards the formation of a special defense strategy for the Indonesian cyber army (Soewardi, 2013).

Internet is a global media with great potential to dominate all activities in this world. The existence of the internet plays a very important role in world communication and dissemination of information. The emergence of the internet also allows humans to enjoy two realms in life, namely, the real world and the virtual world. Along with the development of technology in cyberspace, it will have a negative impact on a country, especially on cyber security practices. At the moment, cyber crime, cyber violence and cyber warfare that occur in cyberspace also have a major impact on the physical sphere, which can threaten national harmony and security. The latest data shows that cyber threats are increasingly occurring globally, including in Indonesia, in which it has became a target for hackers. It has been reported that the hackers of foreign origin have attemped to get access to the cyberspace of Indonesia's corporate sectors as well as conducting espionage activities.

These cyber attacks indicate that Indonesia's cybersecurity system is ineffective, most probably due to the limited law policies and enforcement have been implemented. Indeed, only the Information and Electronic Transactions Law (UU ITE) applies in Indonesia to govern its cyberspace issues. This regulation still does not cover the handling of tapping practices in the world or e-commerce governance. Recognizing the importance of cybersecurity in the development and welfare of the country, Cybersecurity Indonesia continues to lead the cybersecurity industry in Indonesia by being actively involved in various strategies at various levels of the state. In addition, various efforts by the Indonesian government to overcome cyber threats are carried out, one of which is by implementing securities against cyber threats. This shows Cybersecurity Indonesia's strong commitment in empowering cybersecurity.

Although we have been made efforts to combat cyber threats, they are still unavoidable and are still happening, therefore to optimize the implementation efforts, the issued regulations require additional materials and elaborations on implementation strategies, cooperation model, and

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

organization. In addition, implementing national cyber defense needs to strengthen their defense by using a securitization. Securitization does not necessarily mean developing a capacity to fight but means that the sector is made a matter of national security. The securitization of cyberspace involves a history of the information technology domain, the potential as an offensive tool for the military and the acceptance of potential vulnerabilities of a state. Once the state recognizes the potential offensive use of cyber-threats, and its own vulnerabilities to attacks it becomes a matter of national security. Therefore, militarization could occur due to securitization, once cyberspace represents a threat or problem to national security governments could then develop an offensive capacity.

The key objective of this paper is to examine the extent to which actions have been taken by the Ministery of Defence of Indonesia in cyber threat securitization processes. This paper also seeks to examine the impact of that cyber threat securitization process to ensure the security of the Indonesia's cyber space.

2. Literature Review and Analytical Framework

Securitization is a step taken, outside the established rules of the game, and frames security issues as a special type of politics or above politics (Buzan et al., 1998). This view can be interpreted to mean that securitization is a process and perspective of state political authorities in understanding, perceiving, and implementing a security issue with a high threat category because it is beyond reasonable limits, where political decisions regarding security are taken because of the presence of security threats that are special.

Securitization studies aim to understand "who carries out securitization (securitizing actor), on what threat issues (existential threats), for whom (referent object), why, with what results, and at least under what conditions" (Buzan et al., 1998). The securitizing actor proposes a definition of security in which he describes the threat (existential threat), the legitimate security provider (legitimate security provide), the reference object (referent object), and the legitimate means (legitimate means) to deal with the problem (Baysal, 2020). The threat of a Referent object does not create securitization, only a securitizing move. To successfully securitize an issue, the securitizing actor must carry out a securitizing move that is accepted by the audience as terms of securitization. Furthermore, an existential threat can in principle be anything that can threaten the security of a reference object (Erwin & Tadjdeh, 2012). Then, Referent objects are objects that appear to be existentially threatened and have a legitimate claim to survive. Traditionally, the reference object can be a part of the country which includes the government, region and society (Baysal, 2020).

A view that is not much different was also expressed by Lieven (2020) that securitization begins with a speech act about a particular threat, by an authoritative national leader, institution or party. The speech acts conveyed try to divert the threat from normal politics into a security issue, thereby legitimizing extraordinary measures to overcome the threat. Securitization is a rule-governed practice, its success does not necessarily depend on the existence of a real threat, but on the discursive ability to effectively provide development with a certain pattern" (Balzacq, 2005). According to Emmers (2018), every securitization consists of a security measure (with speaking the language of security and calling for the implementation of extraordinary countermeasures) and political action (a

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

political decision to articulate a threat in such a way as a way to reassure target audiences).

3. Methods

This paper adopted qualitative resarch method. Creswell (2009) defines qualitative research method as a method used to explore social phenomena using inductive analysis, various data sources, and flexible research designs, where the researcher is the key actor in the research. This research utilised desciptive qualitative approach which framed within the context of non-traditional security approach, particularly that of securitization theory. The key role of researchers in qualitative research is the researcher's interpretation of the phenomenon under study and the researchers' interpretation of the problem through the use of relevant theories to produce holistic explanations (able to describe complex social phenomena) (Creswell, 2009).

Research using qualitative methods was chosen because this method is suitable for explaining complex social phenomenon and qualitative methods are adaptive and flexible so it is suitable for explaining contemporary phenomena. This method is also compatible with the wishes of the researcher where the main focus of the qualitative research method is the individual meaning of a phenomenon, so through this study the researchers attempted to be the party who understand the reality that occurs (Creswell, 2009).

4. Results and Discussion

4.1. Doctrine of State Defense and Cyber Security

The State Defense Doctrine states that the implementation of state defense must be placed on three fundamental aspects which are the goals of national defense, namely covering aspects of state sovereignty, territorial integrity of the Republic of Indonesia, and the safety and honor of the nation. Cyber attacks can interfere with state sovereignty because the party carrying out the attack can see state secret data and eavesdrop on the conversations of state officials such as the president and ministers. In addition, cyber attacks can damage the safety and honor of the nation because cyber attacks can damage the country's economic system and create chaos on the official government website (Ministry of Defense, 2007).

For this reason, the Indonesian government needs to build a national cyber defense system that can ward off these threats. This is in accordance with the deterrence function contained in the Indonesian Defense Doctrine which states that the embodiment of defense efforts of all national forces which have a psychological effect to prevent and eliminate any threats, both from outside and that arise within the country, to the sovereignty, territorial integrity of the Republic of Indonesia and the salvation of all nations. The character of deterrence is that it is not passive, but actively undertakes defense efforts through efforts to build and foster the country's ability and deterrence, both militarily and non-military. The deterrence function is carried out with a deterrence strategy that rests on deterrence instruments in the form of political, economic, psychological, socio-cultural, technological, and military instruments (Ministry of Defense, 2007).

Determination is the most fundamental substance of the defense strategy (Asia Centre, 2018). Modern defense strategy is not just how the country's defense efforts to destroy the enemy, but how to create conditions that affect potential opponents to discourage attack. Determination efforts were directed to as much as possible to build the impression for potential opponents that

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

attacking Indonesia would lead to failure. Based on this case, the Government of the Republic of Indonesia through the Ministry of Defense issued a policy to build a cyber defense system in Indonesia. This defense system is planned to not only have defensive properties, but also can be used for offensive purposes. To build a cyber defense system, the Ministry of Defense needs to carry out a process of securitization on this issue so that all elements of the country accept and support the cyber defense system policy (Asia Centre, 2018).

4.2. Speech Act by The Minister of Defense of The Republic of Indonesia

Speech Act is an action taken by Securitizing Actor to influence the relevant audience so that they believe in the ideas / concepts initiated by Securitizing Actor (Buzan, Weaver, and de Wilde, 1998). In the context of securitization, the speech act is carried out so that the audience believes that an issue that was not previously a security issue should be made a security issue because this issue requires extraordinary actions in handling it. In the context of cybperspace in Indonesia, the Ministry of Defense as a state institution that focuses on the idea of military involvement in securing cyberspace is the securitizing main actor who most often carries out speech acts. Minister of Defense of the Republic of Indonesia, Purnomo Yusgiantoro, was the figure who most frequently conveyed the importance of cyber defense for Indonesia. The Minister of Defense often gives statements in the mass media and becomes a speaker at seminars where the Minister of Defense emphasizes the importance of developing a very strong cyber defense for Indonesia (Republika, 2013).

> *"Cyber attacks that can interfere with the sovereignty of the nation are currently wide open. Cyber army will consist of military, non-military and formed to ward off these attacks. We plan to form a cyber army. Every year we do cyber competitions and there are those who are specialized for defense or attack.".*

On the pages of the English-language national newspaper, the Jakarta Post, a statement by Minister of Defense Purnomo Yusgiantoro was also found, as follows (Rulistia, 2014):

> *"Cyber threats can be asymmetrical, where conflicts take place between one nation, whose cyber unit is developing, and another nation's, whose is already very advanced, to anticipate this, we are now strengthening the defense force by developing our own cyber defense. The center is located at the Defense Ministry's headquarters in Pondok Labu, South Jakarta. It operates as part of the ministry's data and information unit. The COC will be at the frontlines. The system will be connected to the TNI [Indonesian Army] and individual cyber units in the Army, Navy, Air Force and the ministry. The center is divided into teams that had specific tasks such as intrusion prevention, threat analysis, hacker monitoring, recovery and attack. From the center, we now know the kind of attacks that occur every day in Indonesia. We analyze the situation and developments, and I get the reports on which cyber attack that needs to be watched carefully and what we should do about it, COC was still a new initiative that needed work to develop. We only have around four*

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

to five skilled operators in each division, still far from the ideal 20.".

"We are also forming a cyber-army. Every year we do this for cyber. Defence threats are not only traditional, (but) also for non-traditional ones. We prepare troops that have been sent to several countries, I can't say where, to attack and defend, in the future, the military militants' joint there we will be formed. The commanders are two stars, three stars, cyber is not a hacker, a cracker, we are also improving the satellite-based communication system. Later this is very important to support the existence of these cyber troops.".

The speech act delivered by the Minister of Defense shows a conclusion that the increasing current level of cyber technology has been accompanied by an increase in the vulnerability of cybercrime and cyber attacks or cyberwar both in quality and quantity. In order to achieve the hope of being able to overcome and cope with all cyber attacks,the Ministry of Defense and the TNI have taken the initiative to build cyber defense forces in the military domain which have been continuously developed to date.

4.3. Act of Securitization by Securitizing Actors and Functional Actors

On October 23rd, 2020, the Ministry of Defense formed a task force called the Cyber Operation Team. This team is chaired by the Director General of Defense Potential, Dr. Ir Pos M. Hutabarat, whose members are units related to the Ministry of Defense, other related state institutions outside the Ministry of Defense, and academics from varies universities.

The main task of this Task Force is in policy formulation on the matter concerning to capacity and capability building of cyber defence in Indonesia. In addition, the Task Force is also responsible in designing cyber defense capability policy in the areas of human resources, regulations and technology. The Task Force has also produced the Grand Design Cyber Defense. The document is a national strategic road map for cyber defense which contains the draft of the minister of defense regulations to form a CoC (Cyber Operation Center), drafting presidential regulations regarding structurel organizations that deal with cyber defense issues at national level, information security within the Ministry of Defense/TNI, and administration of domain names within the Ministry of Defense/TNI. The national cyber defense strategy roadmap was established o serve as a guide in developing and building cyber defense capabilities as an attempt to have effective regulations, good organizational structures, modern and reliable infrastructure, and fostering the potential of existing human resources for a strong and sustainable cyber defense capability.

It is hoped that national capacity building with regards to improve national resilience to tackle various cyber-attacks will be further enhanced with the formation of the grand design for the National Cyber Defense in 2013. At the same time, infrastructure development also needs to be improved, especially within the Ministry of Defense and other state institutions. The existing capabilities, such as APJII, ID SIRTI, ID CERT and others can be considered as basic capital in the context of concept preparation and initial development or a comprehensive Backbone Cyber Defense, considering that the development of the Cyber Defense concept is still sectoral, and not an integrated unit of National Cyber Defense (Arianto & Anggraini, 2019).

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

One of the results of the work of the Cyber World Working Team is the issuance of Minister of Defense Regulation No. 86 of 2014 concerning Guidelines for Cyber Defense. Based on this regulation, a special unit named COC (Cyber Operation Center) has been established. The Cyber Operation Center is one of the work units under the Ministry of Defense's Data and Information Center which has the task of maintaining vital infrastructure and cyber attacks, and so, there are several labs such as monitoring labs, digital forensic, electrical, network, malwere, and simulation have been developed (Kemhan, 2017). COC is in charge to run all the procedures and decisions been made by the previous task force. This includes on the matter concerning to technology infrastructure preparedness, human resources and regulations. COC is filled by personnel who are experts in the field of information and communication technology. COC's organizationa structure consists of several parts, namely the prevention section, the analysis of the form of threats, the monitoring of threats or disturbances, the repair and recovery section, the attack section and the administration team. In addition, the COC is also in charge of developing, constructing and maintaining cyber defense infrastructure within the Ministry of Defense. COC is also responsible in giving awareness of the threats of cyberspace within the context of Ministry of Defense.

In addition to these main functions, COC or better known as Pushansiber also has an organizational structure that is based on 3 main areas: (1) areas of governance and cooperation in charge of structostructing and defense cooperation including cyber governance, cooperation, planning, implementation and cyber maintenance; (2) Working areas of cyber operations (Technical policy preparation in the field of cyber operations including monitoring, analysis and reporting of cyber threats, bullying, digital forensics and recovery, carry out cyber operations including monitoring, analysis and reporting of cyber threats, bullying, digital forensics and recovery, monitoring, evaluation, control and reporting in the field of cyber operations, and Establishment of Computer Emergency Response Team (CERT) in order to respond to cyberattacks, as well as monitoring and evaluation in each cert task implementation); (3) The field of security guarantor is tasked with implementing the guarantor of cyber defense security from external threats.

Even though the COC is currently operating, the resources owned by the COC are still insufficient when referring to the ideal number that should exist. On that basis, the Ministry of Defense also held a competition called the Cyber Defense Competition in 2015. This competition consists of two categories, namely general and student categories. Through this competition, the Ministry of Defense obtained several advantages. First, the Ministry of Defense obtained data on the number of human resources who are experts in the field of hacking in Indonesia. Second, it becomes a yardstick for measuring the ability of military personnel serving in the cyber field (the Ministry of Defense provides training to military personnel who have skills in the field of ICT). Third, it becomes a place of socialization regarding the importance of the state to have a strong cyber defense capability. And finally, it becomes an event for the Ministry of Defense to recruit talents from all over Indonesia to join and dedicate their expertise to the country.

The success of securitization can be seen from the consent given by the relevant audience to the perceptions triggered by the securitizing actor. In the case of cyber securitization, the Ministry of Defense conducted a speech act through various statements in online media. The success of securitization can also be seen from the

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

agreement in the point of view among the subjects themselves. In this study, the researchers saw that subjects in government such as the DPR have the same view as the Ministry of Defense that cyberspace threats are real.Subjects outside of government in the form of non-governmental organizations such as FTII (Indonesian Information Technology Federation) also agree with the perceptions developed by the Ministry of Defense. This is evidenced by the participation of FTII in developing cyber defense. FTII is involved in FGD (Focus Group Discussion), workshops, and training with the Ministry of Defense in the process of building cyber defense capabilities by the Ministry of Defense. A total of twelve experts from FTII were also participated when asked by the Ministry of Defense to become resource persons for their expertise in the field of information and communication technology (Kompas, 2013).

FTII as a functional actor has also collaborated with the Ministry of Defense in terms of providing human resources who will be assigned to operate cyber defense units at the Ministry of Defense. The Cyber Defense Competition (CDC) program initiated by the Ministry of Defense also involved FTII as a collaborative partner in the implementation of the program. Not only FTII, CDC is also a collaborative arena for several actors who are experts in the field of information and communication technology, including ID-SIRTII, Nawala, Xirka, Inixindo, and D-Net.

The product of this securitization is COC. Success can also be seen from whether the presence of COC has eliminated threats and covered up existing vulnerabilities. According to a statement from the Ministry of Defense itself, the COC is arguably a successful policy when the operations of the COC itself have been able to withstand attacks that targetting the Ministry of Defense. However, COC has several drawbacks. First, the COC was formed on the basis of a law in the form of a Minister of Defense Regulation, meaning that the scope of authority, duties and functions of the COC was limited to the Ministry of Defense and the TNI. The COC does not have the authority to protect state institutions other than the Ministry of Defense. Second, the COC is not a structural organization. Because it is not a structural organization, the COC does not have a POP (*Organizational Principles and Procedures*) so that its position, authority and accountability are still unclear.

5. Conclusions and Recommendations

The Indonesian government, in this case the Ministry of Defense, has taken securitization measures against cyberspace. The Ministry of Defense has identified cyber threats attacking the ministry and Indonesia' cyberspace. In conducting securitization in the cyber sector, the Ministry of Defense has made speech act efforts to relevant audiences in Indonesia. This is specially toward internet users by providing various statements regarding the importance of building cyber defense capacity and capabilities by the government, particularly by the military in a country. Therefore, the Ministry of Defense takes charge and seeks to build a special unit with strong cyber defense capability an instituion that the country has yet to establish. The absence of this institution makes Indonesia vulnerable when facing cyber attacks. Currently, there are several institutions that have duties and functions in the cyberspace area such as ID-SIRTII, Lemsaneg, and Polri, but all three do not have the authority to carry out comprehensive defense efforts against all types of cyber attacks.

The Ministry of Defense formed a task force that aims to prepare emergency measures to deal with further dangers The role of this Task Force isto prepare plans for the development of cyber defense capabilities

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

within the Ministry of Defense. COC is one of the work results of this task force. The COC is claimed to be a success of this securitization process, whereby, the COC is operational and has the ability to prevent all attacks against the Ministry of Defense. In its efforts to establish COC, the Ministry of Defense has succeeded in collaborating with functional actors, namely FTII. FTII plays its part by sending experts in the field of information and communication technology to become resource persons at the Ministry of Defense.

The Ministry of Defense also created other programs that support capacity building and capabilities of cyber defense in Indonesia. One of the requirements for a strong cyber defense capability is the existence of quality human resources. Because the Ministry of Defense currently lacks human resources who are experts in this field, the Ministry of Defense is looking for talents to be further trained through the CDC. In the implementation process, CDC is also supported by several functional actors such as FTII, Nawala, Xirka and D-Net. CDC is a tool for the Ministry of Defense to seek talent, as a media for socialization and a training arena for military personnel to test their abilities. However, COC has several drawbacks. The basis for the formation of the COC in the form of Permenhan No. 86 of 2014 on Guidelines for Cyber Defense makes the authority of the COC only within the Ministry of Defense, not on a national scale. The COC does not have the power to deter attacks against other Indonesian government institutions.

References

Book Reference:

Betz, D. J. 2011. *Cyberspace and the State; Toward a strategy for cyber-power*. London: Routledge.

Broadhurst, R. G., & Chang, L. Y. 2013. *Cybercrime in Asia: Trends and Challenges*.

Buzan, B., & Lene Hansen. 2009. *The Evolution of International Security Studies*. New York: Cambridge University Press.

Buzan, B., Woever, O., & Wilde, J. De. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers Inc.

Caballero, M & Anthony. 2016. *An Introduction to Non-Traditional Security Studies: A Transnational Approach*. London: SAGE Publications.

Creswell, J. W. 2009. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.

Gultom, R. 2019. *Cyber Warfare Sudah Siapkan Kita Menghadapinya*. Bogor: Unhan Press.

Lieven, A. 2020. *Climate change and the nation state: the realist case*. Allen Lane.

Book Chapter:

Emmers, R. 2018. "Securitization". In *Contemporary Security Studies* (pp. 173–188). Oxford University Press. https://doi.org/https://doi.org/10.1093/HEPL/9780198804109.003.0012.

Journal:

Arianto, A. R., & Anggraini, G. 2019. "Building Indonesia's National Cyber Defense And Security To Face The Global Cyber Threats Through Indonesia Security incident Response Team On Internet Infrastructure (Id-Sirtii)", in *Jurnal Pertahanan & Bela Negara*, 9(1), 17.

Balzacq, T. 2005. "The Three Faces of Securitization: Political Agency,

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

Audience and Context", in *European Journal of International Relations*, *11*(2), 171–201. https://doi.org/10.1177/1354066105052960.

Baysal, B. 2020. "20 Years of Securitization: Strengths, Limitations and A New Dual Framework", in *Uluslararası İlişkiler / International Relations*, *17*(67), 3–20. https://www.jstor.org/stable/26928568.

Kello, L. 2013. "The Meaning of Cyber Revolution: Perils to Theory and Statecraft", in *International Security*. Vol. 38. No. 2. pp: 7 – 40.

Khanisa. 2013. "A Secure Connection: Finding The Form of ASEAN Cyber Security Cooperation", in *Centre for Political Studies, Indonesia Institute of Science*. pp.41-53.

Putra, D. A., Saragih, H. J. R., & Deksino, G. R. 2020. "Implementasi Manajemen Risiko Pertahanan Siber Kementerian Pertahanan untuk Mendukung Pertahanan Negara", in *Manajemen Pertahanan: Jurnal Pemikiran dan Penelitian Manajemen Pertahanan*, *6*(1), 100–121. https://jurnalprodi.idu.ac.id/index.php/MP/article/view/594.

Rahmawati, I. 2017. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) in Peningkatan Cyber Defense", in *Jurnal Pertahanan dan Bela Negara*. Vol 7, No.2, 2017, pp 51-66.

Roztocki, N., Soja, P., Weistroffer, & Roland, H. 2019. "The role of information and communication technologies in socioeconomic development: towards a multi-dimensional framework", in *Information Technology for Development*, *25*(2), 171–183. https://doi.org/10.1080/02681102.2019.1596654.

Sa'diyah, N.K. 2017. "Rekontruksi Pembentukan Nasional Cyber Defense Sebagai Upaya Mempertahanakan Kedaulatan Negara", in *Jurnal Perspektif*, Volume XXI no 3, 2017, Pp 168-187.

Triwahyuni, D & Wulandari. 2016. "Strategi Keselamatan Cyber Amerika Serikat", in *Jurnal Ilmu Politik dan Komunikasi*. Vol. VI No.1/Juni. pp 107 – 118.

Widjajanto, A. 2005. "Evolusi Doktrin Pertahanan Indonesia", in *Jurnal Pro Patria.*

Yani, M. Y., & Rizal, M. 2016. "Cybersecurity Policy and Its Implementation in Indonesia", in *ASEAN Studies*, pp. 62-75.

Online Source:

Badan Instalasi Strategis Pertahanan (Defense Strategic Installation Agency). 2017, in *https://www.kemhan.go.id/bainstrahan/category/berita-pushansiber/page/3*, accessed at October 10th 2020.

Erwin, S. I., & Tadjdeh, Y. 2012. "Top Five Threats to National Security in the Coming Decade", in www.nationaldefensemagazine.org: *https://www.nationaldefensemagazine.org/articles/2012/11/1/2012november-top-five-threats-to-national-security-in-the-coming-decade*.

ITU. 2015. "Global Cybersecurity Index & Cyberwellness Profiles", in ITU-ABI Research.

Kementerian Pertahanan Republik Indonesia, 2007.

Kementerian Pertahanan Republik Indonesia, 2008.

Kementerian Pertahanan Republik Indonesia, 2017.

Kompas. 2013. "Kemhan: Ancaman Non Militer Meningkat", in *https://nasional.kompas.com/read/201*

Global Political Studies Journal
Volume 8 Nomor 2 Edisi Oktober 2024
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v8i2

3/04/26/02165814/kemhan.ancaman.nonmiliter.meningkat, accessed at August 24th 2020.

Nugraha, A. 2019. "Personal Communication". May 12, 2019.

Republika. 2013. "Pemerintah Akan Segera Bentuk Cyber Army", in *https://republika.co.id/berita/nasional/politik/13/09/24/mtmg89-pemerintah-akan-segera-bentuk-cyber-army*, accessed at September 14th 2020.

Rulistia, N. 2014. "Creating an Embryonic Cyber Defence Force", in *Jakarta Post*: *http://www.thejakartapost.com/news/2014/05/25/creating-embryonic-cyber-defense-force.html*, accessed at August 10th 2019.

Soewardi, B. 2013. "Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defence) Yang Tangguh Bagi Indonesia", in *Media Informasi DITJEN POTHAN KEMHAN*.

Ulum, M. 2017. "Cyber Security and Defence Policy of Indonesia", in *https://www.researchgate.net/publication/326155837_Policy_Brief_Recommendation_Cyber_Security_and_Defence_Policy_of_Indonesia*, accessed at August 10th 2020.

Research Report (Thesis/Disertation):

Asia Centre. 2018. "Cybersecurity in Southeast Asia", 3-9.