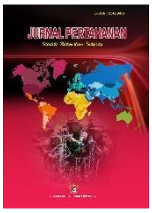
Jurnal Pertahanan

Media Informasi tentang Kajian dan Strategi Pertahanan
yang Mengedepankan *Identity*, *Nationalism* dan *Integrity*
e-ISSN: 2549-9459
http://jurnal.idu.ac.id/index.php/DefenseJournal



STRENGTHENING THE CYBER DEFENSE CENTER OF THE MINISTRY OF DEFENCE OF THE REPUBLIC OF INDONESIA (PUSDATIN KEMHAN) TO SUPPORT THE INDONESIAN DEFENSE DIPLOMACY IN CYBER DEFENSE SECURITY COOPERATION IN ASEAN

Rifani Agnes Eka Wahyuni[1], Surryanto Djoko Waluyo[2], Haposan Simatupang[3]
Indonesia Defense University
IPSC Area, Sentul, Sukahati, Citereup, Bogor, West Java, Indonesia 16810
rifaniagnes@gmail.com[1], surryantodw_kemhan@yahoo.com[2], tupang2007@yahoo.com[3]

Article Info

Article history:
Received : February 11, 2020
Revised : October 27, 2021
Accepted : December 27, 2021

Keywords:
ADMM Plus,
Confidence Building Measures,
Cyber Defense Security,
Defense Diplomacy,
National Defense Information System

DOI:
http://dx.doi.org/10.33172/jp.v7i3.747

Abstract

The development of information technology in the international world impacts cyberspace, covering all aspects of national life. So, the government must understand the condition of cyber security in Indonesia and build a national defense system to overcome various threats that come through cyberspace. ASEAN has become one of the platforms for Indonesia to fight for its national interests to support national security in the cyber field. The purpose of this research is to analyze the efforts to strengthen the national defense system based on five aspects of cybersecurity capacity building to realize Indonesia's defense development in cyber defense security through the role of Cyber Defense Center as an actor in Indonesia's defense diplomacy in enhancing cyber defense security cooperation in ASEAN. These strategies and efforts were analyzed through a qualitative approach, and primary data were collected through interviews with informants from various government agencies. In addition, literature, journals, and related documents are also used as supporting data. These efforts resulted in an agreement in the form of making a cyber-portal between countries and equality of view to continue to conduct cybersecurity training in the form of seminars and workshops to build the capacity of the national defense system.

INTRODUCTION

Cybersecurity has now become a significant concern of international relations in various ways. In the middle of the spread of the technology to hacking fast, many countries and international organizations focus more on preparing security measures and promoting multilateral cooperation to counter the threat of cyber. Cybersecurity can be as devastating as a physical military attack so that the state is required to make adjustments in the national defense. The constellation issue of Traditional security issues for Non-Traditional security is cybersecurity.

Based on a report issued by the Poneman Institute in 2018 showing that cyber threats and the availability of enabling technology will continue to have the most significant impact on the overall state of cybersecurity (Lieberthal & Singer, 2012), as indicated that fulfillment costs are expected to have a lower impact. On the other hand, organizational factors such as the integration of third parties into internal networks and the inability to recruit and retain qualified human resources are expected to have a greater impact on the overall state of cybersecurity.

Specifically, the United States and China, as two world powers in the 21st century, are facing each other on the issue of cybersecurity in the form of hacking and espionage. They are trying to build a global framework for Internet governance, where cybersecurity is one of the sub-controversial fields, but their consensus has not been framed (Lieberthal & Singer, 2012). It was marked that since 2013 the United Nations Group of Governmental Experts (UN-GGE) Forum, a global cyber governance organization, was formed by the United Nations. Indonesia has been a member since 2017. At that time, the UN-GGE Forum focused on the country's actions to respond to cyberattacks. Countries belonging to The North Atlantic Treaty Organization (NATO) proposed that cyber-attacks could be synchronized with conventional military attacks.

But the proposal did not meet an agreement. Eventually, the UN-GGE Forum was split into two blocks. In 2019 member states again agreed to discuss Global Issues of Norms and Behavior in Cyberspace. The United States and Russia have submitted resolutions to be debated at the 2019 UN-GGE General Meeting. In general, the United States and its allies want the disclosure of the Confidence Building Measure (CBM) to measure and find out the cyber capacity of each country. In contrast, the Russian alliance wants the sovereignty of each country in cyberspace (BSSN, 2019).

Forming a network of cybersecurity cooperation is undoubtedly not an easy matter because of the contestation of the paradigm of cyberspace governance among major power states. One of them is reflected in the failure of the UN-GGE to finalize its final report at the United Nations (UN) General Assembly session in June 2017. What hinders them are differences in positions on international humanitarian law, the right to self-defense, and countermeasures that are believed to legitimize the militarization of cyberspace. (Rosandry, 2018). As for building cyber capacity, the countries that have undertaken to build cyber capacity primarily involve the most basic steps, such as through cybercrime laws, increasing law enforcement capabilities, or creating emergency response teams commonly called the Computer Emergency Response Team (CERT). In developed countries, cybersecurity capacity building has also developed strategies to protect critical infrastructure and form organizations that are specifically responsible for Cyber Security issues.

Various efforts to build Indonesia's cyber capacity are carried out in various ways, one of which is that Indonesia's diplomacy in the field of cyber has been active. In the multilateral forum, Indonesia discussed cyber norms, specifically the UN-GGE as a forum for UN member states in maintaining information security. Indonesia also actively participates in the discussing working groups formed by UNODC to develop guidelines for dealing with Cybercrime with the scope of prevention, international cooperation, and capacity development (Alam, 2017). Indonesia believes that national capacity building and international cooperation will intensify a governmental and public policy that is more binding and relevant in dealing with the issue of Cyber Security.

ASEAN member countries are also carrying out capacity building of cybersecurity in the regional scope because they consider this quite urgent. It is proven by conducting discussions on cyber security in various discussions in one of the political and security cooperation forums called the Association of Southeast Asian Nation Regional Forum (ARF) and Expert Working Group at the ASEAN Defense Ministry Meeting (ADMM) Plus. ADMM Plus is a meeting of a high-ranking official in this matter, the Minister of Defense of ASEAN countries and related countries, to discuss issues related to security in the ASEAN region.

ASEAN first handled the cyber issue in 2012 in the ASEAN Regional Forum (ARF) and subsequently developed a work plan to promote cooperation and build trust. Subsequently, in 2015, a high-level conference (Summit) ASEAN ministers about security all cyber (cybersecurity). Within the regional scope, the adoption of the ASEAN 2017 Declaration to Prevent and Combat Cybercrime is essential because, for the first time, ASEAN has a unanimous decision on Cybercrime. The success of the ASEAN project is a step in building confidence (Confidence Building Measures/CBM). ASEAN has identified 11 (eleven) areas in its work plan, and ARF has also compiled a list in its work plan. ASEAN can strengthen law enforcement through capacity building in joint and digital forensic investigations among ASEAN law enforcement agencies. ASEAN has created a master plan to promote the development of information and communication technology in each ASEAN country.

As one of the ASEAN member countries, Indonesia has also been making various efforts for a long time to build the capacity of cybersecurity. It is partly due to many Indonesian internet users, which in 2017 reached 132,7 million. As one of the highest internet user countries in the world, Indonesia is also not free from cyber-attacks. The Indonesia Security Incident Response Team on the Internet Infrastructure Coordinator Center noted that during 2017 Indonesia experienced around 205 million cyber-attacks (IDSRTII Report, 2018). Meanwhile, data from the Ministry of Communication and Information shows that the health, financial, education, and government institutions are the most vulnerable to being targeted by cyberattacks (Swastanto, 2016).

As stated by the Director-General of Directorate General of Defense Strategy, Ministry of Defense *(Strahan Kemhan)* for the 2015-2017 period, it was stated that the cyber-attack was in the form of a WannaCry virus infection that had attacked almost the entire world. More than 100,000 networks in 150 countries are infected with the ransomware-type virus, causing huge losses (Swastanto, 2016). This cyber-attack is an impact or anomaly from the development of information technology that has become the daily needs of the world community. This cyber-attack is expected to occur and continue to the new system or network.

In addition, the rise of various cyber threats in Indonesia made the government formulate various policies to overcome these problems. The next element in building cybersecurity capacity in Indonesia is the organizational structure. The handling of cybersecurity is still sectoral because every one of ministry had their own such for example, regarding censorship of negative content in the cyber world, it is the task of the Ministry of Communication and Information, related to hate speech, the Ministry of Communication and Information will also intersect with the Indonesian Police. Hunting for digital criminals (cybercriminals) carried out by the Cyber Crimes Unit at the National Police Headquarters on the defense side will intersect with the Ministry of Defense, which already has a Cyber Operation Center (COC). There are several jobs handling information security incidents by the Ministry of Foreign Affairs, Handling e-commerce fraud with the Ministry of Industry, Ministry of Trade, and the Ministry of Communication and Information. Then, counter-terrorism by National Counter Terrorism Agency (BNPT), intelligent cyber operations with Indonesian State Intelligence Agency (BIN), financial crimes, and the digital economy by Financial Transaction Reports and Analysis Centre (PPATK) and the Corruption Eradication Commission (KPK). Which makes this matter not coordinated in an integrated manner, which makes overlapping authority.

In Indonesia at this time through the Indonesian Ministry of Defense itself has formed an institution related to cyber defense, namely the Cyber Defense Center (Pushansiber), as an element of carrying out the duties and functions of the Defense Ministry's Strategic Defense installation body which has the task of carrying out governance, cooperation, operations, and *cyber* defense security guarantees. As stated in Minister of Defense Regulation (*Permenhan*) 14 of 2019 concerning the Organization and Work Procedure of the Ministry of Defense, the main task of cyber defense is to cope with cyber-attacks that cause interference with the country's administration. This regulation is used as a guide or reference for the preparation, development, and application of cyber defense within the Ministry of Defense. Pushansiber is expected to be at the forefront of efforts to prevent the threat of cyber-attacks. It needs a capacity of cybersecurity Indonesia to develop the country's defense.

The readiness to increase Indonesia's cyber capacity in dealing with security threats and Cybercrime is undoubtedly very dependent on national policies and interests in strengthening the country's information defense system through the Ministry of Defense's Pushansiber to be effective in carrying out Indonesia's cyber capacity building particularly for regional areas in ASEAN because ASEAN itself has various cyber-related meetings, one of which is through ADMM. The key lies in partnership and the existence of a comprehensive national strategy. First, partnerships in the context of international cooperation are inevitable. No country can face cyber threats without international cooperation, given the nature of the threat of Cybercrime that is cross-country and complex. With Indonesia's strategic position that can attract major powers in the field of cyber commitments in ASEAN, Pushansiber is expected to encourage the same global understanding in multilateral forums, in this case, ADMM-EWG, and bridge the paradigm contestation and differences in interests among the ASEAN region.

Second, Pushansiber partnerships with stakeholders at the national level such as the Ministry of Communication and Information, National Cyber and Crypto Agency (BSSN), the National Police, the State Intelligence Agency, the Ministry of Foreign Affairs, and others. Ongoing and consistent collaboration is essential in supporting Indonesia's defense diplomacy in handling cyber issues. Third, the national strategy in the cyber field is needed to reinforce the orientation of Indonesia's foreign policy and diplomacy.

Some things that become obstacles for realizing the strengthening of the country's information defense system through Pushansiber in supporting Indonesia's Defense Diplomacy in ASEAN include internal and external aspects. There are problems in the internal aspect, such as the absence of a national cybersecurity policy. In contrast, the external aspect is the lack of a visible role of Pushansiber in developing cyber capacity in the ASEAN region regarding cybersecurity.

Cybersecurity, which was initially only part of the widening issue of threats, later became critical in developing a country's defense. The Indonesian government, through Pushansiber, actually has the opportunity to carry out Indonesian Defense

Diplomacy. It is embodied in cybersecurity cooperation to support strengthening the national defense information system in defining Indonesia's defense diplomacy position and strategy in ASEAN. It enhances Indonesia's international role in the global cyber constellation as a form of protecting national interests and building Indonesia's defense.

Therefore, Pushansiber needs to be developed in various aspects of the cybersecurity component, including in policymaking and cooperation, to build the capability of Indonesia's defense information system. Based on this background, the purpose of this research is to analyze the efforts to strengthen the national defense information system to realize Indonesia's defense development in cybersecurity through the role of Pushansiber as an actor in Indonesia's defense diplomacy in enhancing cybersecurity cooperation in ASEAN.

METHODS

This study uses qualitative methods, namely verbal descriptions with sentences conveyed by the resource person. Then the analysis used is descriptive, meaning research to find out something in depth from a descriptive point of view to analyze an event factually and accurately. The time used is cross-sectoral, using phenomena at a particular time, explorative, descriptive, or explanatory (Sugiyono, 2009). Cross-sectional research can explain the relationship between one variable and another so that its implementation will be related to the government with the defense aspect. Therefore, the case study method is carried out intensively, in detail, and in-depth on a particular symptom or phenomenon with a narrower scope so that it is more specific and will facilitate researchers in conducting research. Even though the scope is narrow, the dimensions explored must be broad, covering various aspects so that no one aspect is overlooked. As a qualitative research variant, case study research emphasizes the depth of the subject rather than a large number of subjects studied.

As with the nature of qualitative research methods in general, the case study method should also be carried out on ongoing events or symptoms. Not a symptom or event that has been completed or *ex post facto* (Rahardjo, 2010). Soy explains the process or six steps for conducting a case study; determine research questions, exceptional cases and determine data collection and analysis, preparation for data collection, data collection, evaluation and analysis, and reporting (Soy, 1997).

In this study, data collection was done through the interview method. Interviews are conducted by asking questions that require answers orally or in writing through question and answer while face to face between the researcher and the respondent or the person being interviewed. The interview is the most effective data collection technique to find out and obtain accurate information to support research. In addition, it is also accompanied by documentation, namely the collection of printed data in the form of introductory notes, policy formulations, legal rules, resolutions, and agreements, including literature sources, dictionaries, magazines, newspapers, and other relevant sources of information for use in research (Sugiyono, 2017). Unit of analysis in this study are informants who have competence in providing information related to their field of work, namely Head of Data and Information Center of the Ministry of Defense of the Republic of Indonesia Head of Sub-Directorate for Drafting Basic National Defense Policies at the Directorate General of Defense of the Ministry of Defense (*Sunjakdas Hanneg*) Ministry of Defense of the Republic of Indonesia; Head of the Governance and Cooperation Division of the Ministry of Defense of the Republic of Indonesia; Director of Control, Information, Investigation and Digital Forensics of the National Cyber and Crypto

Agency of the Republic of Indonesia; and Academics.

This study uses the case study method, considering that the focus and sub-focus that we examined will coincide with some instances within a certain period in this study. The data analysis technique used is precise, directed to answer the problem formulation or test the hypothesis formulated in the proposal (Sugiyono, 2017). The purpose of data analysis is to solve research problems, show the relationship between the phenomena variables contained in the study, provide answers to the hypotheses proposed in the study, as material for making conclusions and implications and suggestions that are useful for further research policies (Hasan, 2010).

Cybersecurity, which at first only became part of the widening of the issue of threats, later became one of the critical focuses of attention in developing a country's defense. Therefore, the Indonesian government, through Pushansiber, actually has the opportunity to conduct Indonesian Defense Diplomacy in the cybersecurity collaboration to support strengthening the national defense information system.

Defense diplomacy for CBM is carried out to reduce tensions and eliminate negative perspectives so that relations between countries run well. In addition, CBM is needed to show the transparency of defense policy so that one country is not considered a threat by another country (Acharya, 2014). In this case, defense diplomacy for CBM is carried out in state visits, information exchanges, dialogues and consultations, declaration of strategic cooperation, and military cooperation. They define the position and strategy of Indonesia's defense diplomacy in ASEAN, enhancing Indonesia's international role in the global cyber constellation to protect national interests and build Indonesia's defense.

RESULT AND DISCUSSION

Strengthening the National Defense in Cyber Security

Each state in its formation history is seen as a human association. In this case, the people who live and work together to pursue a common goal, in this case, the ultimate goal of each country is to create happiness for its people as stated by Harold J. Laski, "Creating conditions where people can achieve their desires to the fullest" (Budiardjo, 2003).

Likewise, Indonesia's National Goal is to protect all Indonesians and all Indonesian blood, promote public welfare, educate the nation's life, and participate in carrying out world order based on freedom, eternal peace, and social justice. To achieve this, we attribute it to the national interest, Law 3/2002 stipulates that our national interest is to maintain the unified country of the Republic of Indonesia based on the 1945 Constitution and Pancasila and ensure the smooth progress of the country's development and to achieve national goals. While Indonesia's dynamic national interests are in tune with the phenomenon of world development, national security and national development are strongly influenced by the dynamics of strategic environmental changes and domestic factors such as political dynamics and interaction between communities. Cyber defense is an attempt to cope with the attack of cyber that disrupts the national defense. The application of cyber defense is a priority obligation for the state and all agencies as mandated by Law 3/2002 on the National Defense System that the government must prepare and implement in a total, integrated, directed, and continuous manner to uphold state sovereignty, territorial integrity and national safety from all threats, including cyber threats. The level of importance is directly proportional to the level of dependence on the use of Information and Communication Technology (ICT). It causes the Ministry of

Defense or Indonesia Armed Forces (TNI) to be obliged to take essential cyber defense steps, both within their environment and to support the cross-sectoral cyber defense.

The Term of Cyber Defense, firstly used in the DOD Joint Publication 3-12, where the USA Government called Defense Cyber Operation (DCO). DCO is "Cyberspace Operations (CO) intended to defend DOD or other friendly cyberspace … (and) are passive and active cyberspace defense operations to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems." (US Joint Staff, 2018). Because the ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and the response action is critical to enabling unity of effort in successfully detecting and defending against advanced cyber-attacks, cyber-defense needs to be carried out in a planned and integrated manner so that its application can run precisely and optimally.

Protection is a mechanism to safeguard strategic assets and information resources from various potential attacks through cyberspace. In the context of cyber defense, protection is a preventive step taken by related institutions as part of a risk mitigation strategy against various existing threats. Various studies and research confirmed that a holistic approach needs to be used in building the concept of protection. Cyber-based defense systems must be carried out by building cybersecurity on three main elements: human, process, and technology. As explained earlier, cybersecurity is built on five work areas, namely legal certainty, procedural actions, organizational structure, capacity building, and international cooperation (Ardiyanti, 2016).

Firstly, in the aspect of legal certainty, it can be seen that Indonesia, to meet the national interests of cybersecurity, has accommodated on Minister of Defense Regulation No. 14 of 2019 concerning the organization and functioning of the Ministry of Defense. As well as the rules of procedure had been covering the policy division of duties of the work unit of the Ministry of defense in the ability of cyber complete, which includes the ability in deterrence, repression, and recovery to overcome cyber threats. On one side also includes issuing presidential decree No. 133 of 2018 regarding BSSN. However, the Minister of Defense Regulation and Presidential Decree also do not contain a complete set of managerial and technical competence standards, procedural standards, and working mechanisms in the cyber field that fully integrates the workforce incorporated in the system of study and guidance. Of course, it will result in delays in the capacity building of cybersecurity Indonesia. The delay shows that the formulation of the Ministry of Defense competency policy as an element of supporting the implementation of the duties and functions of the Ministry of Defense in cyber defense is not yet complete.

The next aspect in building cybersecurity capacity is procedural action which consists of a framework and strategy regarding cybersecurity. Suppose you look at this aspect, Indonesia, which is still formulating strategies and policies in cybersecurity until now. It results in each institution's coordination and integration efforts being unfavorable in carrying out cybersecurity. However, the Government of Indonesia gave responsibility to BSSN as a national computer emergency response team (CERT) as a Team in charge of securing cyber networks in Indonesia based on Presidential Decree Number 133/2017, which later had a revision in Article 1 and 2 of Presidential Decree Number 28/2021 that BSSN carries out government duties in the field of cyber security and passwords to assist the President in administering the government, which as a coordinator that duty with another ministry like as the Ministry of Defense (MoD) itself, which MoD had divided between Data and Information Center (Pusdatin) and Cyber

Defense Center (Pushansiber) based on Article 1177 of Minister of Defense Regulation Number 14/2019.

In the aspect of organizational structure, Indonesia has a well-structured institution in cybersecurity. The establishment can see this BSSN as an institution that has the task of coordinating other institutions on cyber issues and the separation of Data and Information Center (Pusdatin) and Cyber Defense Center (Pushansiber) within the Ministry of Defense. ASEAN itself has various cyber-related meetings divided into several sectors. One of them is at the ADMM meeting where the leading actor is the Ministry of Defense, where this role is delegated to cyber pushers. At the same time, the existence of BSSN is involved by the Ministry of Defense in envoys as part of cross-sectoral coordination. Although, to date, the standard procedures of the ministry of defense in coordinating each work unit are still being formulated together with the formulation of the Grand Design Framework for Information and Technology of the ministry of defense's data.

So, at this time, the cybersecurity problem is still not maximizing coordination between institutions. Organizations, therefore, at this stage of the initial conditions of the personnel policy in the field of cyber has not specified aspects of deterrence, enforcement, and recovery. It will be difficult for implementation policy is to set forth the vision, mission, and work program of Data and Information Center (Pusdatin) of Ministry of Defense in cyber. This condition will affect the elaboration of the implementing rules under it.

In the aspect of capacity building, the attention and seriousness of the Government of Indonesia, in this case, Cyber Defense Center (Pushansiber) can be seen through its policy to incorporate cybersecurity awareness into strategic policy. It makes the user or cyber users within the ministry understand and be aware of the cybersecurity issues early on. In addition, Cyber Defense Center (Pushansiber) actively participates in training programs conducted by BSSN in improving students' abilities in cybersecurity issues.

However, the program is still in the form of non-binding appeal. So that the initial conditions of the personnel in the field of cyber both quantitatively and qualitatively still do not follow the list of the personnel (DSP) and a job description based on the competence of human resources in the field of cyber. Paying attention to the actual condition of the personnel will affect the performance of the Pushansiber organization, which in the end, is less able to support the achievement of its main tasks. Therefore, efforts are needed to complete the availability of Human Resources (HR) personnel in the cyber field in terms of quantity and quality.

In the aspect of international cooperation regarding cybersecurity, active Pushansiber participate in international cooperation forums conducted by discussing cybersecurity. However, active participation is still being carried out when implementing HR development policies in the cyber field. It is found that there are difficulties in defining cooperation policies to carry out duties in the field of deterrence, repression, and recovery in the face of cyberattacks. Some policies can only implement containment measures and recovery through cyber defense. Meanwhile, to carry out the enforcement action required a policy on the ability to take action in the form of cyber-attacks.

Due to the lack of quantity and quality of the Pushansiber policy in the network field, Pushansiber activities cannot perform their tasks optimally. Therefore, it is necessary to find a solution to this person's lack by implementing a policy on the development of human resource capabilities in the area of Pushansiber members' abilities, skills, and attitudes in the network field. The human resource capacity development policy predicts that the performance of Pushansiber will be more effective and efficient in achieving the planned goals or the goals of the Pushansiber organization.

Interest development policy strategy is to improve the expected standards of competence and for the organization's benefit to raise productivity. To carry out this HR competency development policy, it is necessary to foster personnel in the cyber field for the fulfillment of cyber personnel through the process of recruitment, selection, provisioning, placement, and improvement of HR quality in the cyber field. In addition, it is also necessary to optimize the coordination and communication space between stakeholders in the Pusdatin environment to cover the lack of quantity and quality of cyber human resources in Pusdatin.

Thus, both conceptually and empirically, the implementation of cybersecurity as a whole, based on five aspects of cybersecurity capacity building. It can be seen that Indonesia, in this case, Pushansiber, still needs to get serious attention from the Government of Indonesia, primarily when referring to the data presented at the beginning that Indonesia was at the top level as a country that is often the target of hacker attacks. So that policy development strategies and competencies in the Ministry of Defense, in this case, are still not optimal to carry out the main tasks and Pushansiber functions in the cyber field.

At this stage of the results, it was found that the achievement of the cybersecurity development policy should be by the duties, authority, and responsibility to carry out the functions of deterrence, repression, and recovery to deal with cyberattacks. The availability of the policy will be explained in more detail in the operational rules for implementation below it. Policy on competency development Pushansiber in the field of cyber can be used as the basis for the placement office under professionalism and proportionate - it is based on the competence of human resources in the field of cyber. Meanwhile, to deal with problems in the field of personnel in the cyber field, it is necessary to have availability of personnel both in quantity and quality. This condition will directly affect the operational implementation of the cyber field's deterrence, prosecution, and recovery tasks. Likewise, the results of managerial competence and technical competence in the cyber field that do not follow competency standards are expected to affect Pushansiber performance.

Indonesia's Defense Diplomacy by Cyber Defense Center (Pushansiber) in Cyber Security Cooperation in ASEAN

The state must respond by increasing awareness of vulnerabilities or threats to information security, sensitive and strategic information. Cybersecurity can guarantee a solid national defense and as a foothold in clarifying the information in public relations communication strategies. Indonesia badly needs the swift development of this technology that can be utilized as a stage of communication, transaction, interaction, and cooperation. This condition erases the conventional paradigm to compete and compete to secure himself and the institution. So, collaboration needs to understand our abilities and limitations from others to synergize and collaborate in that realm.

So, later on in the international cooperation in cybersecurity, Ministry of Defense required other countries to share knowledge related to developing technology and information. The security of cyber itself refers to the dynamic national interests in Indonesia need to handle Non-Traditional Security Issues in the context of cybersecurity do through multilateral diplomacy by bringing this to the ASEAN regional forum through ADMM Plus.

Global security is on every country's agenda because of the very global threat of terrorism at this time. Seeing the dynamics of the development of the strategic environment at a global level also increases various security issues, one of which is the issue of cybersecurity. The source of security threats can be from abroad or foreign governments, hacking communities that are difficult to anticipate, or individuals without community involvement and can be from the mistakes of unscrupulous parties. Collaboration and collaboration within CSIRT are needed to realize cybersecurity.

BSSN has a Gov-CSIRT (Government Cyber Security Incident Response Team), a government sector cyber incident response team that provides incident response services in the government sector. Gov-CSIRT has the mission of building, coordinating, collaborating and operating a system of mitigation, crisis management, prevention, and recovery of cybersecurity incidents in the government sector. So that ASEAN has a solid basis to play a role in this matter through the ADMM to enhance cooperation between ASEAN countries to fight the issue of cybersecurity. The form of diplomacy that can also be developed by Indonesia, in this case, is the concept of defense diplomacy delivered by the Muthanna KA, where defense diplomacy is an ongoing cooperative relationship to build trust, prevent conflict, introduce transparency in defense relations, build perceptions of the public interest, changing mindset of partners, and introducing cooperation in other fields (Muthanna, 2011).

The Ministry of Defense is also in line with that, which explains three types of defense diplomacy, defense diplomacy for Confidence Building Measures (CBM), capacity building or defense capability, and the defense industry. Defense diplomacy for CBM represented by the relationship involvement active Pushansiber in international forums related to cybersecurity held in ASEAN that which is evidenced by the involvement of Pushansiber in the forum ADMM Expert Working Group on Cybersecurity opportunities Indonesian diplomacy to achieve the national interest in the case was able to secure from cyber threat.

So that cooperation needs to be done to understand the capabilities and limitations so that Indonesia can build a policy to synergize and collaborate in fulfilling the development of information and communication systems. The contribution of Indonesia's defense diplomacy in ADMM-EWG CS will be significantly influenced by the environment and the methods used by ADMM-EWG CS and adjusting Indonesia's defense diplomacy strategies adopted in cybersecurity cooperation.

Indonesia's defense diplomacy is used as an instrument to pursue national interests in multilateral diplomatic relations in ASEAN, and defense diplomacy developed to build good relations with other countries to reduce uncertainty with cybersecurity in the regional region. On the other hand, with the understanding that external security conditions and regional stability will significantly influence a country's security conditions, Indonesia's defense diplomacy, which aims to secure its territory, will also contribute to the security of other countries. Furthermore, the success of a country's defense diplomacy strategy is a collaboration of diplomacy, defense, and development components which have three main characteristics: Defense Diplomacy for Confidence Building Measure, Defense Diplomacy for Defense Capabilities, and Defense Diplomacy for Defense Industries. (Syawfi, 2009).

Based on these conditions, the contribution of Indonesian defense diplomacy by Pushansiber in ADMM-EWG CS will be reviewed through each existing character.

Defense Diplomacy for Confidence Building Measures (CBM)

Defense diplomacy for CBM is carried out to reduce tensions and eliminate negative perspectives so that relations between countries run well. In addition, CBM is needed to show the transparency of defense policy so that one country is not considered a threat by another country (Acharya, 2001). In this case, defense diplomacy for CBM is carried out in state visits, information exchanges, dialogues and consultations, declaration of strategic cooperation, and military cooperation.

Pushansiber applies this to participation in Table Top Exercise, a simulation designed to test the theoretical ability to respond to situations in the field of cybersecurity. The Table Top Exercise is expected to support CBM between countries to create a sense of security and mutual trust in cybersecurity. The form of the result of this Table Exercise is the creation of a cyber portal that is useful for Indonesia and other ASEAN Defence Ministers' Meeting Plus Experts' Working Group on Cyber Security (ADMM EWG-CS) countries in sharing information to map cyber incidents, find out potential threats, identify perpetrators, and decide on actions to deal together. It should be understood that not all ADMM EWG-CS member countries have a particular body that deals with cyber issues and their consequences. Several state officials provide personal contact points to Indonesia.

It shows that Indonesia is trusted by other countries in cooperation if there is a cyber incident and is supported by understanding that cyber threat is a threat that can not be handled by one country alone. In addition, participation in creating cyber portals implies the view that ADMM EWG-CS member countries do not want conflicts in cyberspace. Therefore, contact points are needed as a means of communication and diplomacy. It will undoubtedly support the stability of regional security from cyber threats.

The sharing point of contact between countries shows that Indonesia's defense diplomacy aims to reduce the risk of misunderstanding and escalation of tension that leads to conflict. Furthermore, the Indonesian government can use communication media to develop broader cooperation in forming cybersecurity, both nationally and internationally. One thing that needs to be understood about the importance of sharing information in cybersecurity is identifying the perpetrators. It considers that first cyberspace will always involve international networks, but there is no specific policy in the international world regarding cybersecurity. The results of previous studies related to defense diplomacy in fulfilling Cyber Security also found that this condition occurred in Indonesia and ASEAN countries. If the Indonesian government does not immediately form a strategic regulation related to cyber at the national and regional levels, the Indonesian government may adopt international policies. Secondly, one of the major conventions currently underway on cyber issues is the Tallinn Manual which NATO countries have so far formulated.

When the Tallinn Manual gets a joint consensus, both the UN and Indonesia will adopt the regulations in the Tallinn Manual, in whole or in part. Third, in the Tallinn Manual, there is an explanation of the "the use of force" category in cyber operations, one of which states that cyber operations can be categorized as the use of force if it has a critical impact on national interests resulting in damage, destruction, injury, and death (Setyawan & Sumari, 2016). Under these conditions, the ADMM EWG-CS communication forum is important, producing a joint policy on creating a cyber portal. So that if there is a cyber-attack on Indonesia, the government can clarify the relevant country whose location is identified. In addition, if the location of Indonesia is used as a proxy by the real culprit in a cyberattack, then other countries in ASEAN who are victims can make clarifications to Indonesia. It is very important so that the building of mutual trust between countries can avoid the process of accusing each other as perpetrators and being targeted in retaliation for attacks, bearing in mind that, based on the Tallinn Manual, retaliatory attacks may involve military use.

Based on Pushansiber's defense diplomacy contribution and the ADMM EWG-CS mechanism, which aims to contribute to the confidence-building and preventive diplomacy efforts, it is possible to establish aspects of defense diplomacy to form a CBM in ASEAN. On the other hand, the effort made by establishing a contact point network between countries is one of the implementations of mutual trust between countries and one of the preventive measures to increase the escalation of conflict. Thus, the Pushansiber defense diplomacy contribution is in line with the ADMM EWG-CS mechanism and the character of defense diplomacy for confidence-building measures. Furthermore, the challenge that must be faced is how countries with a network of contact points work together and handle cyber incidents.

Defense Diplomacy for Defense Capabilities

The second aspect of defense diplomacy is to build defense capabilities. In contrast to building defense capabilities in general, such as the military component and the number of defense equipment and actors involved in conventional warfare, cybersecurity has a broad aspect by involving various actors.

As defined by the international telecommunication union that cybersecurity is a collection of tools, policies, security concepts, guidelines, approaches, risk management, actions, exercises, best practices, guarantees, and technology that can be used to protect the cyber environment, organizations, assets, and users including computing devices that are connected, personnel, infrastructure, applications, services, telecommunications systems, and everything that is transmitted and/or information stored in the cyber (International Telecommunication Union, 2010) in building cybersecurity or security of the cyber one country, one of the things that became very difficult is to ascertain where the attack originated.

Unlike conventional attacks such as missile launches that leave a trace and can be tracked, parties who use cyber tactics can easily hide their whereabouts. It is because uncertainty is a prominent aspect of cyber conflict concerning the attacker's identity, the scope of collateral damage, and the potential effect on the intended target of the cyber-attack. This condition can be used as a foundation that the development of national cybersecurity capabilities is not only in the form of material but also the exchange of information and development of human resources originating from within (national scope) and from outside, which can involve international cooperation. For example, countries with prior knowledge of cybersecurity can share their knowledge with other countries within global cooperation.

In this case, regional organizations can play their part in making this happen. It was implemented by Indonesia and ADMM EWG CIS countries by conducting various seminars, training, and workshops to share knowledge about cybersecurity. In addition, in concrete form as a solution to improve the internet network's defense and security capabilities in ASEAN. Pushansiber also uses ADMM-EWG CS to update and share cybersecurity information. For example, knowledge of botnet malware. The malware program is considered dangerous because it can use computers from other parties in large numbers to carry out attacks without being noticed by its users. Through forums, workshops, and seminars, the government can quickly get information and anticipate it quickly.

Defense diplomacy as part of defense capability is also carried out to strengthen the national defense materially. However, the ADMM-EWG CS mechanism that tends to dialogue and consultation, and information exchange makes it difficult to establish a form of cooperation to build defense capacity in the cyber field that is material, such as defense equipment and other defense components. Therefore, contributions made by Indonesia and other countries tend to develop information, knowledge, and human resource development. On the other hand, the results of the ADMM EWG-CS can be used as input for making national policies in cybersecurity. Thus, the cooperation established in ADMM EWG-CS to build material defense capability is not intended to form an agreement such as the purchase of defense equipment but as an entry point to seek standard views and open up more effective forms of cooperation.

Defense Diplomacy for Defense Industries

One aspect that has not been able to be met by Pushansiber in conducting Indonesian defense diplomacy through ADMM EWG-CS is defense diplomacy for the defense industry. Some obstacles are the availability of infrastructure and the strategy of building the strength of the defense industry that deals with cyber issues. So, there is no precise mapping of how cyberspace will be applied in the defense industry. In addition, Indonesia does not have an extensive industry engaged in cyber and contributes to defense. Therefore, it becomes difficult for the Indonesian government to map cybersecurity needs in the industrial sphere. Implementing Indonesia's defense diplomacy to build a defense industry is also tricky in the ARF. There are still many ASEAN countries looking for forms in making cybersecurity.

As explained earlier, some ARF countries have different views on understanding cybersecurity. On the other hand, the issue of cybersecurity has not been a significant concern for some members of ADMM EWG-CS due to differences in cybersecurity capabilities. It is what later led to the needs of the defense industry of each country in different cyber aspects. One of the collaborations that need to be pursued by the Indonesian government is the development of information because it is essential in supporting cyber existence. So that it can be concluded in supporting cybersecurity in ASEAN, it should strengthen cooperation by increasing capacity-building efforts among various platforms of the three ASEAN pillars so that ASEAN efforts are focused, effective, and holistically coordinated in the problem of cybercrime. ASEAN must establish a cybersecurity program by working together to defend and take advantage of the region's collective resources. Trust and resilience are the main points for policymakers and non-state actors to raise awareness about cybersecurity. They also adopt an active defense attitude by using all ASEAN forums such as the ARF and AMCC.

The contribution of Indonesia's defense diplomacy by Pushansiber will be significantly influenced by the environment and the methods used by Pushansiber, and the adjustment of Indonesia's defense strategy implemented in Cyber Security cooperation in ASEAN. Indonesia's defense diplomacy is used as an instrument to pursue national interests in defense diplomacy relations developed to build good relations with other countries to reduce uncertainty about cybersecurity in the regional region. On the other hand, the understanding that the security conditions will be significantly influenced by the external security and stability of the region. Especially diplomatic efforts top developing a policy on cybersecurity conducted by the Indonesian government to provide legal certainty and capacity building of cybersecurity in action procedural that therein consists of frameworks and strategies regarding cybersecurity.

CONCLUSIONS, RECOMMENDATIONS AND LIMITATION

Indonesia enhances the national defense information systems through Pushansiber Defense Diplomacy in realizing cooperation in cybersecurity in ASEAN for national defense construction. This study concluded that the defense diplomacy between Indonesia and ASEAN in the cybersecurity cooperation had run well but had not been carried out optimally. Furthermore, researchers will try to elaborate these conclusions more concisely, namely as the relationship between operational mechanisms related to cyber policies in terms of protection, the concept of security, and the process of paralysis of cyber-attacks are aligned. It means that the stronger the operational protection mechanism, the security concept, and the paralysis process, the more robust the national defense system is in the face of cyber-attacks. Conversely, the weaker the operational protection mechanism, the security concept, and the paralysis process, the weaker the national defense system is in dealing with cyber-attacks.

Thus, both conceptually and empirically, the implementation of cybersecurity implementation. Overall, based on five aspects of cybersecurity capacity building, it can be seen that Indonesia, in this case, Pushansiber, still needs to get serious attention from the Government of Indonesia. Mainly when referring to the data presented initially, Indonesia is at the top level as a country that often becomes a target of hacker attacks. So, policy the development of strategies and competencies in the Ministry of Defense in this regard is still not optimal to perform basic tasks and functions Pushansiber in cyber. The contribution of Indonesia's defense diplomacy by Pushansiber will be significantly influenced by the environment and the methods used by Pushansiber and adjustments to Indonesia's defense diplomacy applied in cybersecurity cooperation in ASEAN.

Indonesia's defense diplomacy is used as an instrument to pursue national interests in defense diplomacy relations developed to build good relations with other countries to reduce uncertainty concerning cybersecurity in the regional region. On the other hand, they understand that external security conditions and regional stability will significantly influence a country's security conditions, especially diplomatic efforts to develop policies in cybersecurity carried out by the Indonesian government by providing legal certainty and building cybersecurity capacity in procedural actions which consist of from the framework and strategies regarding cybersecurity.

REFERENCES

Acharya, A. (2014). *Constructing a Security Community in Southeast Asia* (Second edi). Routledge. https://doi.org/10.4324/9781315796673

Alam, S. (2017). Kemlu Beri Perhatian Serius pada Diplomasi Siber - Peristiwa. Retrieved April 15, 2021, from Nasional Peristiwa website: https://rri.co.id/nasional/peristiwa/429783/kemlu-beri-perhatian-serius-pada-diplomasi-siber

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1), 98. https://doi.org/10.22212/jp.v5i1.336

BSSN, B. H. dan H. M. (2019, January 17). BSSN Berharap Dubes Menjadi Mata dan Telinga Indonesia. Retrieved February 19, 2020, from Info Terkii website: https://bssn.go.id/bssn-berharap-dubes-menjadi-mata-dan-telinga-indonesia/

Budiardjo, M. (2003). *Dasar-Dasar Ilmu Politik*. Jakarta: Gramedia pustaka utama.

Hasan, I. (2010). *Analisis Data Penelitian Dengan Statistik* (5th ed.). Jakarta: Bumi Aksara.

International Telecommunication Union. (2010). Landmark decisions from Guadalajara. Retrieved December 5, 2020, from ITU NEWS website: https://www.itu.int/net/itunews/issues/2010/09/20.aspx

Lieberthal, K., & Singer, P. W. (2012). Cybersecurity and U.S.-China Relations. In *Brookings Institue* (1st ed.). Washington DC: The Brookings Institution. Retrieved from The Brookings Institution website:

https://www.brookings.edu/research/cybersecurity-and-u-s-china-relations/

Muthanna, K. A. (2011). Military diplomacy. *Journal of Defence Studies*, *5*(1), 1–15. Retrieved from http://www.idsa.in/system/files/jds_5_1_kamuthanna.pdf

Rahardjo, H. M. (2010, May 7). Mengenal Lebih Jauh Tentang Studi Kasus. Retrieved April 15, 2019, from https://www.uin-malang.ac.id/r/100501/mengenal-lebih-jauh-tentang-studi-kasus.html

Rosandry, I. (2018). Merajut Diplomasi Siber Indonesia. Retrieved from Media Indonesia website: https://mediaindonesia.com/opini/199360/merajut-diplomasi-siber-indonesia

Setyawan, D. P., & Sumari, A. D. W. (2016). Diplomasi Pertahanan Indonesia Dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum on Cybersecurity Initiatives. *Jurnal Penelitian Politik*, *13*(1), 1–20.

Soy, S. K. (1997). The Case Study as a Research Method. Retrieved March 25, 2021, from https://course.ccs.neu.edu/isu692/readings/l391d1b.htm

Sugiyono, M. P. P. (2009). *Kualitatif, dan R&D*. Bandung: Alfabeta.

Sugiyono, P. D. (2017). *Metode Penelitian Bisnis: Pendekatan Kuantitatif, Kualitatif, Kombinasi, dan R&D*. Bandung: Alfabeta.

Swastanto, Y. (2017). *Tantangan-Tantangan Pertahanan RI dalam Perkembangan Situasi Keamanan*. Bogor: Universitas Pertahanan Indonesia.

Syawfi, I. (2009). Aktivitas Diplomasi Pertahanan Indonesia Dalam Pemenuhan Tujuan-Tujuan Pertahanan Indonesia (2003-2008). Jakarta: Universitas Indonesia. Retrieved from https://scholar.google.com/scholar?hl=en&as_sdt=0,5&cluster=8343986099920831943

US Joint Staff. (2018). Cyberspace Operations. *Joint Publication 3-12 (R)*, *12*(July), 62. Retrieved from http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150%0Awww.e-publishing.af.mil