ISSN 2744-1741
Defense and Security Studies
Original Research
Vol. 4, 2023, pp.84-93
https://doi.org/10.37868/dss.v4.id244

Analysis of presidential regulations concerning cyber security to bolster defense policy management

Rizky Ramadhianto[1*], Tahan Samuel Lumban Toruan[2], Susaningtyas Nefo Handayani Kertopati[3], Hikmat Zakky Almubaroq[4]
[1,2,4] Republic of Indonesia Defense University, Defense Management Study Program, Indonesia
[3] Republic of Indonesia Defense University, Asymmetric Warfare Study Program, Indonesia

*Corresponding author E-mail: rizkramdht@gmail.com

Received: Aug. 8, 2023
Revised: Oct. 2, 2023
Accepted : Oct. 4, 2023
Online: Oct 9, 2023

Abstract

As a developing country, Indonesia must effectively manage its national defense by implementing defense policies which can be interpreted as management activities that transform into defense policy management entities. The objective is to protect against various dangerous threats resulting from the dynamics of the current strategic environment, which continues to undergo rapid and significant changes. Cyber threats pose a potentially dangerous threat that has a multidimensional impact. Therefore, this article analyzes one of the Indonesian government's efforts to deal with cyber threats, which is in the form of Presidential Regulation No. 47 of 2023. The research employs a qualitative descriptive approach in the field of literacy studies, drawing on reputable sources such as journals, books, and internet materials. It investigates the management measures and strategies implemented by Indonesia to combat cyber threats in accordance with presidential regulations for cybersecurity. These findings elaborate on the implementation of presidential regulations that concentrate on cyber crisis management and national cyber security strategy as a suitable and praiseworthy response to the constantly evolving cyber threats. Nonetheless, addressing several challenges requires strategic competencies in leadership to formulate cyber defense policies and strategies and carry them out optimally..

Keywords: Presidential Regulations; Defense Policy Management; Cyber Crisis; Analysis; Cyber Security

1. Introduction

Indonesia, as one of the world's largest countries, possesses abundant national resources, which can bolster or jeopardize the national defense system if not managed proficiently and with suitable strategies. To avert potential threats, it is crucial to implement effective and reliable defense management, which ensures optimal deployment of national forces. Defense management is crucial for the development of defense policies that necessitate an appropriate and sustainable planning mechanism [1]. Defense management refers to a country's ability to effectively and efficiently manage its resources to serve national defense interests in a strategic and comprehensive manner, in accordance with management principles. This encompasses both short and long-term strategies aimed at increasing efficiency and effectiveness.

The management of national defense includes planning, organizing, coordinating, commanding, and

controlling activities at the strategic and policy levels, without subjective evaluations. Defense management at the defense policy level involves managing defense development policies, defense empowerment policies, defense force deployment policies, defense regulatory policies, defense budget policies, and defense oversight policies [2].

As defense management falls under the purview of strategic management, the policy-making process involves developing pertinent defense policies and strategies that address the current and prospective strategic landscape. Alterations or developments in the strategic environment, influenced by values held within a nation's territory, inevitably impact the country's national interests. Therefore, maintaining national security and upholding sovereignty and integrity are key priorities for each country, as they adapt to their unique national interests. National interests stem from two primary factors - they can be rationally demanded because of necessity or changed due to circumstances. Thus, a country's national interests are critical in effectively countering threats evaluated through the dynamics of the strategic environment [3].

With reference to the development of the current strategic environment dynamics which continues to experience rapid and massive changes, as a country, Indonesia at present and in the future will not be separated from challenges, threats, disturbances, and obstacles that are increasingly complex, where the current threat model it has a broad scope and is undergoing a fundamental evolution. If in the past, threats were primarily related to conflicts between nations or threats to national territorial integrity, today's threats are multidimensional in nature, affecting numerous sectors and sub-sectors. Cyber warfare is a multidimensional threat due to its potential danger being equivalent to that of kinetic weapons. The cyberspace revolution must be factored into national security and resilience efforts [4].

Based on data from the Global Cybersecurity Outlook 2023 report by the World Economic Forum, cyber-crime by both state and non-state actors is rapidly evolving to take advantage of changes in a target country's political, technological, and regulatory landscape. This is done through a complex scope creation mechanism that includes volume as a new type of attack, resulting in an acceleration of cyber threats that outpaces the ability to counteract them [5]. Additionally, the European Union Agency for Cybersecurity (2023) predicts that 2030 will mark the pinnacle of the growing cyber threats of today's age. This begins with bottlenecks in the supply chain and reliance on software, to campaigns spreading disinformation and digital surveillance that threatens privacy. Furthermore, inadequate analysis and control, vulnerable infrastructure, advanced hybrid threats, and the misuse of Artificial Intelligence technologies all contribute to this issue [6].

Figure 1. Emerging Cyber-security Threats

Source: ENISA (2023) [6]

On the other hand, according to the 2022 study conducted by the International Institute for Strategic Studies (IISS), Indonesia must move up to at least the second tier as it currently remains in the lowest - third tier [7]. The 2022 National Cyber Security Index positions Indonesia at 47th, classified as being in the weak category, with a score of 38.96 out of 100 [8]. This rank places Indonesia at the third lowest position within the G20 countries.

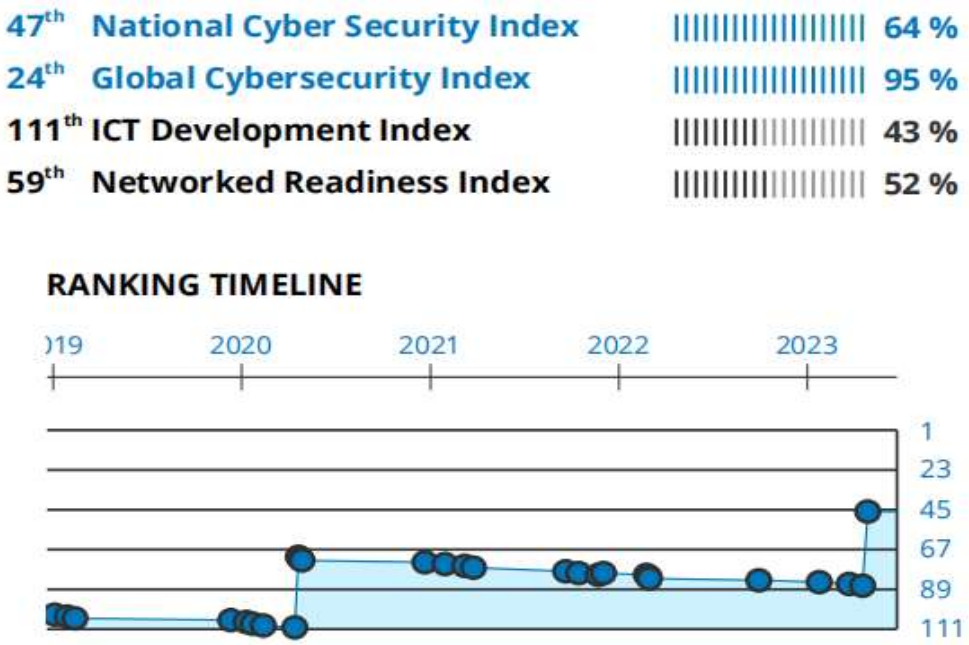

Figure 2. Indonesia's Cyber Security Index
Source: E-Governance Academy Foundation (2022)

As a country aspiring to become the fourth largest global economic power, Indonesia must invest in its cyber sector to enhance its cyber capabilities. Currently, compared to other developing countries, the Indonesian government prioritizes cyber surveillance for domestic security more than cyber security and the use of digital technologies. Although there were institutional changes related to cyber within the armed forces in 2014, at that time no military cyber strategy or doctrine had been developed. However, the first formal strategy for civil-sector cyber security emerged in 2018 [7].

If it is not seriously anticipated through the strengthtening cyber policy by the government, then incidents caused by cyber-attacks like data leakage due to hacking can continue to recur in the governmental institutions in Indonesia. Cybersecurity policy encompasses all aspects of digital data exchange, including Internet usage, data privacy, network usage, and cyber defense. As with any policy, cybersecurity policy must strike a balance between necessary regulations and social freedoms [9]. Cybersecurity policies should prioritize addressing the legal gaps that emerge when cyber policies are overly concentrated on regulating individuals, in order to avoid any redundancy with existing regulations [10].

The government's capacity to respond to cyber threats is restricted and is likely to fail without collaboration with other parties involved in the process [11]. Developing a national cybersecurity strategy involves coordination across governmental and non-governmental entities, as well as the public and private sectors. This collaboration is essential to meet the challenge effectively.

An assessment of the effectiveness of a cyber defense strategy can be conducted by examining the initiatives taken by the governments of the United Kingdom and the United States, two prominent Western powers. The UK is implementing an adaptive and responsive approach by increasing investment in creating a futuristic cyber domain that involves all segments of the country [12]. Additionally, the UK government recognizes the significance of actively addressing the cyber dependencies of adversaries to ensure security in cyberspace.

Meanwhile, the transition of presidential administrations and political parties from the Trump to Biden era in the United States has presented challenges for cyber policies, which are often limited by established conceptual, political, and strategic commitments [13]. Policymakers have approached each policy by interpreting cyber threats with a focus on improving efficiency and effectiveness, rather than implementing radically new strategic or policy approaches .

Based on the comparison between cyber defense strategies as exemplified, eventually this article will analyze one of the Indonesian government's efforts to address cyber threats through regulations, specifically Presidential Regulation No. 47 of 2023 [14] on the cyber security. This regulation intends to bolster policy management in the realm of defense, particularly in cyber defense. In this manner, administrative institutions and stakeholders of the state can attain cyber power and competence, fostering trustworthy and preventing cyber threats for stable and secure cyber security, thus serving Indonesia's national interests.

The research in this article addresses the need to respond to the increasingly complex and crucial dynamics of cyber threats in regard to national security. As the first cyber regulation released by the Indonesian government, this study aims to analyze the management framework and identify the strategies utilized by Indonesia to ward off cyber threats and provide insight for future cyber regulations.

Considering the recent release of this presidential regulation, this article holds significant value as a reference for future cyber studies and a potential source for policy recommendations. Unlike what has been done by Armencheva (2015) examines the factors impacting cyber policies and strategies in European Union (EU) countries, while Niedermeier (2017) evaluates national cyber defense strategies in Central-Eastern Europe. In this article, we analyze Indonesia's national cyber policy framework, with a focus on crisis management and indicators of cybersecurity strategy.

This article can provide valuable policy recommendations for the government and produce effective outcomes for stakeholders in the field of cyber defense, thereby strengthening Indonesia's defense capabilities. The research outcomes can also serve as a reference for academics and defense practitioners to enhance their understanding of defense management discipline.

2. Research method

This study employs a qualitative approach with a descriptive analysis methodology. Qualitative research investigates individuals' lives, histories, behaviors, and the functioning of organizations, social movements, or kinship relationships to uncover findings that cannot be attained through statistical procedures or quantitative methods [15]. The study employs qualitative and empirical methods to examine the scope of cyber security regulations set forth by the Indonesian presidency, with the aim of enhancing the management of defense policy.

Data collection techniques in qualitative research include observation, interviews, document analysis, and audio-visual materials. Document analysis is a method of collecting data in qualitative research that involves analyzing public documents, such as newspapers and official reports, or private materials, such as personal journals, electronic letters, and letters. Meanwhile, audio-visual materials referenced in qualitative research for data collection take on the form of photographs, art objects, videos, or sounds [16].

The research process necessitates time and adaptability, resulting in the definition of the research impacting the research design and methodology, which must also be flexible. The researcher opted for a qualitative approach after thoroughly gathering data from numerous information sources, including academic journals, books, and credible online sources.

3. Results and discussion

Tracing the history, it is evident that the cyber sector in Indonesia lacks strong institutions, coordination, and legal foundations due to the absence of a national strategy. This is primarily a result of inadequate attention to

cyber policy in Indonesia. Initially, the Indonesian government prioritized cyber affairs when it broadened the reach of cyber defense to encompass the concept of total defense [17]. This was subsequently accompanied by augmenting the number of personnel in the National Police of the Republic of Indonesia's (Polri) cyber-crime units from 40 to 100 [18]. Also, the National Crypto Agency was renamed as the National Cyber and Crypto Agency (BSSN).

After re-organizing, BSSN implemented a new role and released a national cyber security strategy that prioritizes cyber resilience, ensuring the security of public services, enforcing cyber laws, promoting a culture of cyber security, and protecting cyber security in the digital economy [19]. The establishment of this national strategy aims to promote global trust and facilitate multi-stakeholder engagement in Indonesia's cyberspace. Additionally, the government focuses on countering domestic terrorism and online extremism in the cyberspace domain.

In 2014, the Ministry of Defense issued guidelines for national cyber defense [20], outlining strategies to prevent cyber attacks that could pose a threat to national defense and high-priority assets, such as private closed networks, telecommunications and banking networks, data centers, online payment systems, and key government assets [21]. Economic national security and domestic instability can be affected by the consequences of cyber threats to national defense. Nonetheless, deficiencies remain in the discussion surrounding the concept of sustained cyber-enabled warfare and efforts towards cyber-offensive tactics, such as enhancing counter-attack capabilities for the purpose of deterrence. Furthermore, the 2015 Defense White Paper positions cyber defense as one of the mainstays of the national defense posture, designating the cyber security function as a core national defense capability that intersects with all other instruments of national power. This integration is accompanied by efforts to modernize the country's cyber capabilities [22].

3.1. National cyber security strategy

The analysis of Presidential Regulations No. 47 of 2023 regarding Cyber Security follows the 'Means, Ways, Ends' theory created by the U. S Army War College. This connection is utilized to protect national interests [23]. Based on this understanding, strategy can be defined as a method of linking potential contributions to achieve specific objectives through the selection of predetermined priorities that consider the greatest impact. Furthermore, it entails the ability to anticipate future developments to effectively manage resources, facilities, and existing infrastructure while using established means.

The government aims to achieve its objectives by defining the scope of cyberspace governance as a domain with the potential to cause sudden strategic impacts on national goals, as outlined in this regulation's 'Ends' aspect. To ensure continuity of the governance system, risk management must also be prepared to anticipate worst-case scenarios. If the government aims to enhance national cybersecurity, it cannot solely concentrate on the internal factors within the country. The government must also take into account external factors that can assist in achieving national interests. Therefore, the government's provisions outlined in this regulation, specifically the exploration of international cooperation between nations and participation in forums and conferences, will undoubtedly enhance the nation's cybersecurity capabilities and serve as a platform for showcasing cyber power to compete on a global level.

The Presidential regulation advocates for the expansion of the national cyber power by bolstering information infrastructure, considering the vulnerability of information to cyber threats. Hence, reinforcing national cyber joints is essential in averting diverse cyber threats that have the potential to disrupt the national cyber order. The next regulation should assess Indonesia's national cyber capability, capacity, and quality. National cryptography receives special attention in the regulation as one potential indicator for creating cyber security policies.

The cyber regulation at hand focuses on strengthening capabilities through various prioritized measures. These measures include optimizing risk identification and analysis, implementing cyber security risk protection measures, enhancing collaboration between stakeholders, increasing the effectiveness of national

cyber security risk mitigation, promoting international cooperation in bilateral, regional, and multilateral forums to foster a safe, peaceful, and open cyberspace. Additionally, efforts are taken to improve the preparation and implementation of cyber policies. Overall, the regulation aims to support and enhance cyber security in a comprehensive and structured manner.

Furthermore, the focus is on technical programs, including cyber crisis contingency plans, emergency response implementation, human resource skills development and implementation, and coordinated and sustainable training programs aimed at increasing awareness of cyber security. These programs aim to strengthen the secure exchange of information and provide high access time. To ensure the uninterrupted implementation of programs stipulated in the regulations, the Indonesian government is taking steps to mitigate potential issues in the cybersecurity sector. This includes the cultivation of laws, raising public awareness of legal matters, and integrated law enforcement measures.

The next aspect to consider is the use of resources to support the implementation of methods in achieving national cybersecurity objectives. These resources comprise people, processes, and technology, forming an ecosystem of critical information infrastructure. In terms of human capital as cybersecurity talent, early childhood education is advisable for the nation's upcoming generation, beginning from elementary to higher education levels. Direct Indonesian cyber experts to engage in scientific research, development, and innovation in the realms of cryptography and technology, in order to bolster national cyber advancement.

Efforts to establish a national cybersecurity infrastructure will undoubtedly impact the strengthening of effective and efficient cybersecurity technology and incident response capabilities, as outlined in government regulations and policy directives prioritizing international cooperation in cyber security. Considering the strategic environmental development, advancements in science and technology, and the five-year national development plan, this endeavor is deemed fitting to back a quantifiable action plan at a national level that outlines and enforces the main areas of concentration in the national cybersecurity strategy.

The matter is crucial for decision-makers and cyber policy analysts to avert misguided attention, for it elevates values as the ultimate goals to be reached, while interests serve as intermediary objectives. Consequently, resultant policies would not aid in achieving national values and could prove detrimental. Assuming the Indonesian scenario is to strengthen fundamental capabilities in responding to cyber warfare challenges, the necessary actions involve changes in the national cyber development paradigm, beginning with personnel and technology, and also incorporating doctrine. The responsibility of policymakers is crucial for implementing the development of cyber defense. By observing divergent perspectives, they can create greater cohesion in cyber security.

3.2. Cyber crisis management

The examination of managing cyber crises is grounded in the management functions theory, which encompasses Planning, Organizing, Commanding, Coordinating, and Controlling. The planning function involves taking the first steps towards achieving a goal, enabling the determination of tactical steps to be taken in the future. The organizing function centers on directing and orienting the division of major tasks at work, with a focus on hierarchy. The commanding function involves directing talent according to the plan in order to achieve work goals in an effective and efficient manner. The coordinating function aligns activities of all units at different levels to achieve objectives. The controlling function serves as the final step in ensuring that the overall management function operates in accordance with goals, standards, and targets by monitoring activities [24]. In analyzing the Indonesian government's handling of cyber crises, these management functions are used as a reference.

During the planning stage, the Indonesian government is encountering obstacles related to their human resources, particularly the cyber skills of their national cyber talents. This is a result of not meeting the minimum standards for cyber security education accreditation, insufficient national funding for cyber security capacity programs, and a lack of formal cyber security education programs, which is evidenced by ad hoc

transfer of knowledge from trained cyber security employees, often involving multiple professional instructors in the field [25]. This situation has prompted speculation that it will take a minimum of two decades or longer for the Indonesian government to establish a self-sufficient cyber defense capability by supplying cyber experts in cyber crisis infrastructure. According to a presidential regulation, there exists a coordinating entity called Electronic System Operators (PSE) responsible for managing cyber crises. The PSE comprises of individuals, state administrators, and business entities, as well as members of the public who independently or collaboratively provide, manage, or use electronic systems for their own or third-party needs [14].

Defense planning has two primary objectives: the first is to attack defense policy, and the second is to ensure flexibility in achieving these objectives. The planning process entails analyzing existing information and data, making predictions, and setting goals. The government aims to proactively handle cyber crisis conditions by implementing a presidential regulation related to cyber security. This involves creating a contingency plan for cyber crisis management, accompanied by a simulation plan using a training and role-play mechanism to prepare for potential scenarios. Socialization of the public is a crucial aspect in the planning stage of cyber crisis management. It is important for individuals to understand a range of cyber threats and techniques needed to mitigate the impact of cyber crises. This process should begin with a community-wide strategy and extend to all levels of Indonesian society.

Organizing involves introducing flexibility while maintaining structural rigidity by reorganizing work processes within an existing framework, rather than restructuring existing organizations. This may include allocating national resources. The cyber security regulations include the formation of a cyber crisis task force organized by the President to address critical issues in cyberspace. The implementation stages executed by the cyber crisis task force are essential to achieving the President's directive for increased structure and systemization.

Commanding involves taking responsibility for decision making and providing direction and guidance to achieve established goals. The function of cyber crisis management is emphasized to ensure efficiency and effectiveness in various techniques and objectives of cybersecurity. Consequently, a commanding role is needed, which is generally carried out by the PSE in terms of following up on early warning information. On the other hand, the President holds the highest authority in providing directives for the national cyber management policy mechanism. Moreover, the President oversees the command flow that is divided into two parts: firstly, the determination of the cyber-crisis status based on the Head of BSSN's proposal, and secondly, the determination to end the cyber-crisis status, based on reports from the cyber-crisis task force.

The analyzed regulations on cyber security by the President indicate that the coordinating function plays the most critical role in managing cyber crises. The analyzed regulations on cyber security by the President indicate that the coordinating function plays the most critical role in managing cyber crises. As the coordinating process governs several other processes, it is expected to have a significant impact on optimizing national cyber security development. Nonetheless, the coordination process requires attention to other factors, notably the establishment of systematic communication between concerned organizations. Organizational communication involves the exchange of messages within a self-contained network. The primary function of organizational communication is to coordinate by disseminating information, emotions, and sentiments [26].

PSE serves as a critical actor in coordinating cyber crisis management efforts with other key components, including the BSSN and state administration agencies. As such, PSE plays a crucial role in optimizing coordination functions. Recently, PSE received an initial report indicating a cyber crisis warning resulting from an escalation of a cyber incident, which subsequently evolved into a full-blown cyber crisis. To respond to cyber incidents and prevent their negative impacts in stages, three levels of Cyber Incident Response Teams were formed: organizational, sectoral, and national. Each team prioritizes integrated elements in all cyber crisis response activities.

Cyber crisis management involves stakeholders coordinating to implement cyber crisis communication protocols and disseminate information to the public. The subsequent step entails carrying out cyber crisis recovery by using a mechanism to restore affected electronic systems and utilizing alternative resources. The objective is to reassess essential and supportive functions to achieve recovery goals, which will be evaluated by recovery time below the maximum limit established in the cyber crisis contingency plan. Furthermore, the quantity of data retrieved based on the predetermined minimum amount of data, alongside the retrieval of essential functions and supporting functions meeting the minimum requirements, serves as an indicator of the recovery process's effectiveness.

The cyber task force presented the President with a comprehensive report consisting of a thorough analysis of their methods in managing cyber crises and their various successful endeavors. They also included recommendations for future actions in handling cyber crises. This stage involves the BSSN function in the post-cyber-crisis period, along with PSE to calculate the estimated value of damages and losses resulting from the cyber crisis. Additionally, they calculate the estimated recovery costs and evaluate the cyber crisis. Calculating the cost of recovery involves replacing the value of damaged assets and estimating the costs needed to restore electronic systems to their pre-cyber crisis state, while also taking into account any economic losses resulting from temporarily damaged assets.

Controlling refers to the practice of regulating activities or programs to ensure they remain on track in achieving predetermined goals. The process involves synchronizing different activities to avoid conflicts, prioritizing time allocation, and enhancing communication. Intervention is necessary during the management of activities and programs to ensure that the focus remains on the goals set within the policy. To achieve efficient and effective cyber crisis management, the controlling function should be strengthened, as current regulations emphasize evaluation activities.

The aim of this operation is to manage the cyber crisis by evaluating the handling of cyber emergencies in alignment with the contingency plan. Furthermore, the expected outcomes are new entities for future consideration in making decisions regarding cyber security policies. However, incompatibility or overlapping between agencies in carrying out their duties can cause hiccups and deviation from the intended direction and function of cyber crisis management. It is crucial to avoid such issues.

4. Conclusions

Defense management plays a critical role in sustaining a nation and its state, particularly in the development of policies and strategies that can be executed in both peacetime and wartime scenarios. Within the framework of defense policy, managerial actions are necessary as decisions concerning defense policies are made by various institutions involved in defense-related fields, including cyber defense.

The establishment of Presidential Regulations No. 47 of 2023 Concerning Cyber Security is a suitable response to the evolving cyber threats and necessary for maintaining cyber security stability. Its aim to address defense policy support elements, such as national cyber security strategy and cyber crisis management, is commendable. However, various challenges must be addressed, beginning with the strength and preparedness of the national cyber-infrastructure required for implementation. This includes the capabilities of national cyber talent and the managerial mechanisms implemented by policy actors, as decision-making in formulating cyber security policies involves stakeholders across sectors.

Therefore, effective strategic leadership is necessary to scan and analyze the strategic impact of cyber threats, identify both potential and factual threats, and formulate cyber defense policies and strategies. Additionally, it is crucial to efficiently and effectively implement the national cyber defense strategy through the execution of defense policy management operations. In the future, a study can explore the strategic leadership model's effectiveness in guiding the vision and mission of national cybersecurity regulations to achieve optimal results.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this research.

Acknowledgments

Many thanks are conveyed to Colonel Air Force Dr. Ir. Hikmat Zakky Almubaroq, S.Pd., M.Si., CIQaR. as Chief of the Defense Management Study Program, for his guidance and inspiration in the completion of this article. Gratitude is also expressed to Major General TNI (Ret.) Dr. Drs. T.S.L.Toruan, M.M., Dipl. SS., CIQaR, and Dr. Susaningtyas Nefo Handayani Kertopati, M.Si. who acted as supervisors for the final coursework and this article.

References

[1] H. Bucur-Marcu, P. Fluri, T. Tagarev, Defence management: An introduction, Geneva Centre for the Democratic Control of Armed Forces, 2009.
[2] M. Supriyatno, Y. Ali, Introduction to Defense Management, Republic of Indonesia Defense University, 2018.
[3] H. J. Morgenthau, Another 'great debate': The national interest of the United States, The American Political Science Review, 1952.
[4] T. S. L. Toruan, Book of National Defense anthologies: Notes of 7 academic soldiers, Aksara Akademia Global Indonesia, 2021.
[5] World Economic Forum, Global cybersecurity outlook 2023, World Economic Forum, 2023.
[6] ENISA, Identifying emerging cyber security threats and challenges for 2030, European Union Agency for Cybersecurity, 2023.
[7] The International Institute for Strategic Studies, Cyber capabilities and national power: a net assessment, The International Institute for Strategic Studies, 2021.
[8] E-Governance Academy Foundation, National cyber security index, E-Governance Academy Foundation, 2022.
[9] Utica University, "What Is Cyber Policy and why is it important?", 2019, (*in press*). https://programs.online.utica.edu/resources/article/what-is-cyber-policy
[10] Dhyta in ELSAM. "Cyber policy reform, the government must determine priorities*",* 2021*, (in press).* https://elsam.or.id/teknologi-dan-ham/reformasi-kebijakan-keamanan-siber--pemerintah-harus-tentukan-prioritas
[11] I. Armencheva, "Aspects of policies and strategies for cyber security in the European Union", *Journal of Defense Resources Management*, vol. 6, no. 2, 2015.
[12] The UK Government, "The national cyber force: responsible cyber power in practice", 2023.
[13] A. Neidermeier, "Same threat, different answer? Comparing and assessing national defence strategies in Central-Eastern Europe", *Security and Defence Quarterly*, vol. 16, no. 3, p. 52-74, 2017.
[14] Minister of State Secretary of the Republic of Indonesia, Presidential regulations of the Republic of Indonesia number 47 of 2023 concerning national cyber security strategy and cyber crisis management, Ministry of State Secretary of the Republic of Indonesia, 2023.
[15] F. Nugrahani, Qualitative research method, Cakra Books, 2014.
[16] J. W. Cresswell, Research design: qualitative, quantitative and mixed methods approaches, SAGE Publications, 2014.

[17] Antara News, “Ministry of Defence encourages non-military defense to become a national program”, *Antara*, 2019, (*in press*). https://www.antaranews.com/berita/860413/kemhan-dorong-pertahanan-nirmiliter-jadi-program-nasional.

[18] M. A. Sapiie, “Police playing tough in combating cybercrimes in Indonesia”, *Jakarta Post*, 2017, (*in press*).https://www.thejakartapost.com/news/2017/02/06/policeplaying-tough-in-combating-cybercrimes-in-indonesia-.html.

[19] National Cyber and Crypto Agency of the Republic of Indonesia, “Indonesian cyber security strategy”, (*in press*). https://bssn.go.id/strategi-keamanan-siber-nasional.

[20] Ministry of Defence of the Republic of Indonesia, Minister of Defense of the Republic of Indonesia regulations number 82 concerning cyber defense, 2014. https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf.

[21] A. R.i Noor, “Indonesian’s strategy to maintain cyber sovereignty”, 2016, (*in press*). https://inet.detik.com/cyberlife/d-3131768/strategi-indonesia-menjaga-kedaulatancyber.

[22] Ministry of Defence of the Republic of Indonesia, “Defence white paper 2015”, pp. 109, 2015. https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIADEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf.

[23] J. B. Bartholomeus, U. S. S. S. I. Army War College, U. S. D. O. N. S. A. S. Army War College, U. S. Army War College guide to national security issues, PA: Strategic Studies Institute, 2012.

[24] D. A. Wren, A. G. Bedeian, and J. D. Breeze, “The foundations of Henri Fayol’s administrative theory”, *Management Decision*, vol. 14, no. 9, p. 906-918, 2002.

[25] Y. Nugraha, “The future of cyber security capacity in Indonesia”, Oxford Internet Institute, 2016. https://ora.ox.ac.uk/objects/uuid:70392ace-4bd6-4066-818e-a3adc1eeedf3.

[26] S. N. H. Kertopati, Communication in security intelligence performance, Gramedia Jakarta, 2013.