Journal of Economics and Business Letters
E-ISSN 2686-6056
P-ISSN 2798-8651
https://doi.org/10.55942/jebl.v5i6.1139

Volume 5
Issue 6
December Edition 2025

Analysis of the implementation of defense economic policy in strengthening cyber capacity in Indonesia

Nurul Faizah Al Khoiriyah*, Suwito, Sri Iswati

Universitas Pertahanan Republik Indonesia, Kawasan IPSC Sentul, Jl. Anyar, Sukahati,
Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810 Indonesia
*e-mail: faizahalkhoiriyah@gmail.com

Received 25 October 2025
Revised 17 December 2025
Accepted 22 December 202

ABSTRACT

Strengthening cyber capacity has become an important component of Indonesia's defense economic framework, along with the development of technology and increasing cyber threats that can affect economic stability and national security. This study aims to analyze the implementation of defense economic policies to strengthen Indonesia’s cyber capacity. The research method used a qualitative approach with a literature study through policy document analysis and budget data, applying George C. Edward III's policy implementation framework which focuses on four key variables: communication, resources, disposition, and bureaucratic structure. The results show that the integration of Indonesia’s defense, economic, and cyber policies has not been fully optimized. The findings indicate that without structural adjustments, the policy will remain normative. Therefore, an adaptive defense economic transformation is needed, placing cyber security as a strategic component by strengthening communication between institutions, increasing investment in human resources and technology, and synergy between defense institutions through bureaucratic simplification.

Keywords: policy implementation, defense economy, cyber defense, national resilience

privietlab.
RESEARCH & PUBLISHING

1. INTRODUCTION

The rapid development of information technology has brought significant changes in various aspects of life, including national security and defense. Traditionally, national defense has focused on the military dimension and conventional weapons; however, cyber threats from cyberspace have emerged as a crucial element that requires strategic attention. Cross-sector cyber-attacks targeting digital infrastructure and strategic economic sectors show that countries need to strengthen their non-military dimensions to respond to threats effectively. In the context of Indonesia, a country with rapid digital economic growth, this challenge is so crucial that it requires strengthening the digital aspect.

In the last five years, the number of cyber-attacks in Indonesia has consistently increased since 2020. Data from SAFEnet (2025) shows that in 2020 there were 147 cyber-attacks in Indonesia, and this number more than doubled in five years to 330 incidents in 2024. This trend indicates an urgent need to enhance cybersecurity enforcement actions. The increase in cyber-attacks reflects the challenges faced by various sectors in Indonesia. See Figure 1

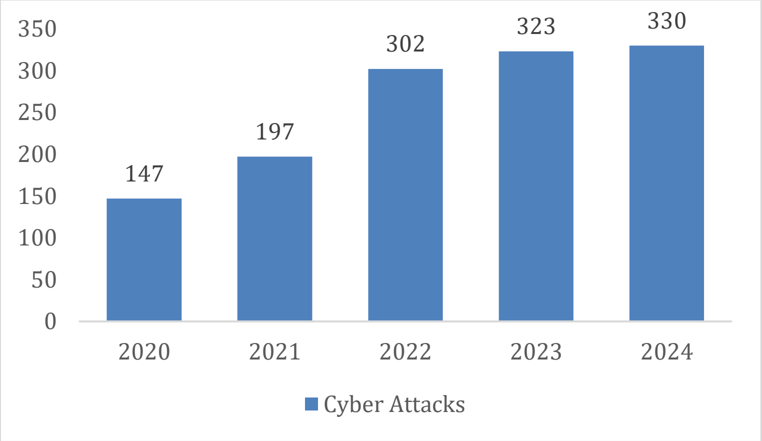

Figure 1. Comparison of Cyber Attacks in the Last Five Years (2020-2024)

Source: SAFEnet (2025)

Cybersecurity issues peaked when a large-scale cyber-attack targeted the National Data Center (PDN) in June 2024. The attack, caused by the Brain Cipher ransomware, had a serious impact on various aspects, such as the loss of access to important data, disruption of public services such as population administration and health services, and damage to information technology infrastructure, including servers and networks, resulting in financial losses. This could also erode public trust in the government's data protection. Furthermore, the government's reputation in the eyes of the international community could also be threatened, and fear of cyber threats could potentially hamper innovation and technological development in the future (Simorangkir et al., 2024). These impacts confirm that Indonesia's national defense system has not yet achieved optimal integration to protect strategic digital assets. Meanwhile, the rapid growth of Indonesia's digital economy requires adaptive defense economic policy instruments to ensure economic stability while strengthening overall national resilience.

Defense economics is defined as a discipline that studies the efficient allocation of state resources to support defense and security interests (Yusgiantoro, 2014). With technological developments, cybersecurity has become integrated into defense economics and is expected to continue growing in the coming years (Gaibulloev et al., 2020). Global North countries such as Israel, Australia, and Singapore have made massive investments to build collaboration platforms between the public and private sectors to protect critical infrastructure, focusing on preventing and mitigating cyber disruptions (Ndubuisi, 2023). However, the integration of defense economics and cybersecurity policies in Indonesia has not yet been systematically formulated. Defense budget allocations are still dominated by the conventional sector, while investment in cybersecurity is relatively limited and fluctuates (Pusat Kajian Akuntabilitas Keuangan

Negara, 2022). This gap raises fundamental questions about the extent to which Indonesia's defense economic policy has been directed at strengthening cyber capabilities.

Thus, this study aims to analyze Indonesia's defense economic policy to strengthen Indonesia's cyber capabilities. Based on the understanding offered by George C. Edward III in his implementation model, this study is analyzed using four main variables, namely communication, resources, disposition, and bureaucratic structure. This theory was chosen because of its relevance in evaluating the obstacles and successes of Indonesia's policy implementation in the context of defense economics and cyber-capacity building.

2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Defense Economics in the Contemporary Security Paradigm

Defense economics is a field of study that optimizes resource allocation between defense needs and other public sectors. According to Yusgiantoro (2014), this concept combines basic economic principles with the unique characteristics of defense, which is public and non-rivalrous, and uses quantitative approaches such as game theory and econometrics to balance military spending with economic growth. This paradigm emphasizes that national security is a prerequisite for achieving economic prosperity. Studies on the economic impact of defense spending examine how budget allocation in this sector affects economic growth, income distribution, and public welfare. On the one hand, high defense spending has the potential to create job opportunities and drive technological advancements. However, on the other hand, such large budget allocations can also cause a diversion of resources from other more productive economic sectors (Sri, 2024).

Furthermore, Hartley (2020) explains that defense economics is a branch of economics that discusses war and peace, which is then expanded to include various aspects of defense economics, conflict, disarmament, and peace. Defense economics applies economic analysis to the defense sector, including the armed forces and the defense industry. This field focuses on decision-making regarding the alternative uses of resources through opportunity costs and behavior that leads to optimization in achieving efficient resource allocation. Along with the dynamics of the times and the global challenges facing the world, the understanding of defense economics has changed. Post-Cold War defense economics is no longer limited to the management of logistical resources during wartime, management of weapons supplies on the battlefield, or strategies for winning wars through control of economic resources. Today, the understanding of defense economics has shifted to issues such as conflict, terrorism, peace, disasters, and other social problems ranging from food to health (Susdarwono, 2020).

In Indonesia, the normative foundation of the defense economic policy is enshrined in Law No. 16 of 2012 on the Defense Industry. This regulation governs not only the technical aspects of the defense industry but also reflects the overall national defense economic policy. Essentially, the defense economy integrates the national security strategy and economic development, involving the allocation of state resources for protection and defense purposes. As explained by Arce (2023), defense economics is part of the public economy. With the development of technology, cyber security has become a crucial element in this field because almost all vital aspects of the state, such as the military, government, and public infrastructure, depend on digital technology, which is vulnerable to cyber-attacks. Thus, strengthening cyber security not only supports national defense but also strengthens the economic dimension of defense.

From this explanation, it can be concluded that defense economics does not only discuss logistics management and war strategy, but is increasingly developing in addressing contemporary issues, including cyber matters. In this context, strengthening cyber capabilities through defense economic policy is a concrete form of adaptive defense development that is in line with the challenges of the digital age and dynamics of modern threats. Thus, the defense economy is not only a means of protecting the country but also a driver of adaptive sustainable development.

2.2 Strengthening Cyber Defense Capabilities

Cyberspace is a place where activities involving the use of information technology and the Internet take place. On the one hand, this space provides many benefits, but on the other hand, it also poses various threats, risks, and disruptions that can range from small to large in scale. Efforts to maintain the confidentiality, integrity, and availability of electronic information and infrastructure in cyberspace so that it remains secure and runs well are referred to as cyber defense (Kementerian Pertahanan RI, 2014). Cyber defense is a collective effort to prevent, detect, and respond in a timely manner to attacks or threats to ensure that no infrastructure or information is damaged and to protect sensitive data and strategic assets amid the increasing volume and complexity of cyber-attacks (Galinec, 2022). Cyber defense not only protects against threats but also improves the use of security resources such as personnel, technology, equipment, and budget to be more effective and efficient (Ahmed et al., 2023). From a defense economics perspective, this ensures that security investments provide maximum results so that the resources and costs used can prevent greater financial and strategic losses.

In Indonesia's defense system, cybersecurity is one of the main pillars of non-military defense, involving the active participation of various stakeholders, such as the government, industry, and society. Cyber threats have become a critical component of modern defense strategies, requiring the development of cyber armies and digital defense infrastructure. In recent years, India, the United States, Indonesia, and China have become the main targets of cyberattacks. Overall, these four countries account for approximately 40% of the total number of reported incidents in the public sector (Yanko et al., 2023). Furthermore, studies show that 63% of global cyber-attacks target critical infrastructure, prompting Indonesia to develop a National Cyber Defense System that is integrated with the Indonesian National Armed Forces (TNI) command system. The Ministry of Defense has expanded the mandate of the Indonesian National Armed Forces (TNI) to include defensive and offensive cyber operations, including strategic data protection and digital counterintelligence (Aditya & Carina, 2025). However, developing a cyber army and digital defense infrastructure requires significant investment. Therefore, the defense economic policy needs to clearly provide funding and regulate fiscal and industrial policies so that capacity building can continue, which is a key factor in the success of the cyber security strengthening program.

2.3 George C. Edward III Policy Implementation Framework

Implementation is defined as the process of interaction between goal-setting and the actions taken to achieve those goals. It consists of planning and organizing the administrative tools and human, financial, material, and technological resources necessary to implement the policy (Kurhayadi, 2023). Policy implementation refers to the actions and processes that connect formal policy decisions with results in the field, namely, a series of activities carried out after the policy is determined by decision-makers.

There are two types of policy implementation models: top-down and bottom-up approaches. The top-down approach used by George C. Edward III in his public policy implementation model is based on the assumption that decisions and directives from the central level must be implemented consistently by lower-level implementers. This theory identifies four main variables that determine the success or failure of public policy implementation (Figure 2).

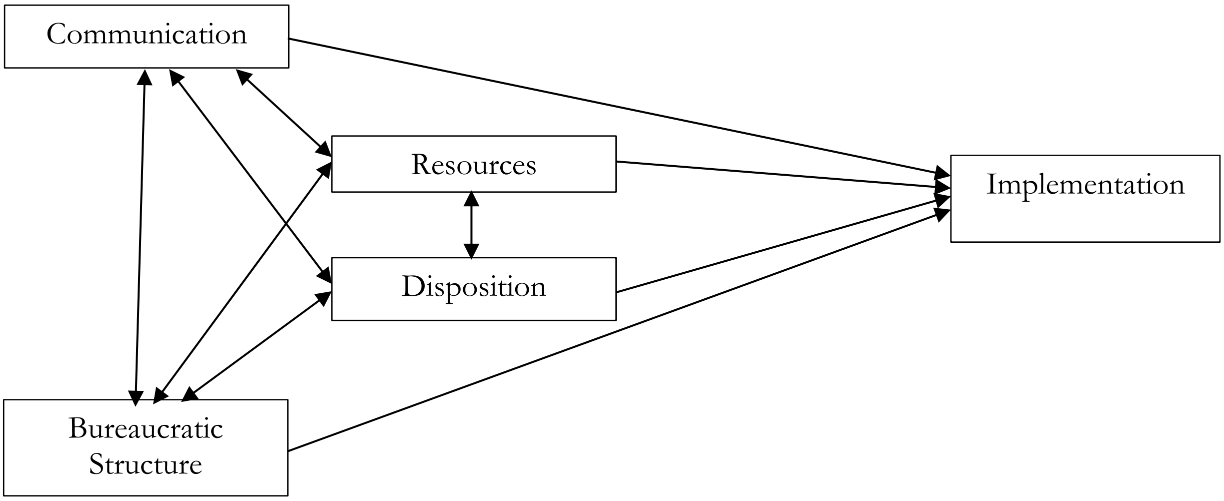

Figure 2. Concepts of Policy Implementation According to George C. Edward III

Source: Edward III (1980)

Edward III explains four main variables that determine the success of public implementation: (1) Communication. Effective communication is important for ensuring successful implementation. Communication refers to the process of conveying clear and effective information between top-level policymakers and field implementers. Without good communication, policies can be misinterpreted or not implemented according to instructions; (2) Resources. Resources include all supporting elements needed to implement policies, such as funds, human resources, materials, and technology. The availability of adequate resources prevents implementation failures owing to a lack of resources. Without adequate resources, policy implementation can be hampered and even fail, even if the policy has been well designed; (3) Disposition. Disposition refers to the willingness, desire, and inclination of policy actors to implement policies seriously and with commitment. Disposition ensures that implementation is not only effective and efficient but also sustainable; (4) Bureaucratic Structure. Bureaucratic structure describes the hierarchical organization within the government, with detailed regulations on the tasks of implementers to ensure structured coordination and avoid overlap in implementation (Edward III, 1980; Saputro & Prakoso, 2021).

3. METHOD

This study uses a qualitative method with a literature review approach. A qualitative approach was chosen to gain an in-depth understanding of the implementation of defense economic policy in the context of strengthening national cyber capacity. A descriptive-analytical approach was used to describe the actual state of cyber security in Indonesia and to analyze the challenges faced. The units of analysis in this study include policy and regulatory documents, such as cyber-related budget reports, cyber defense doctrines, and national cyber security strategies. In addition, this study examines annual reports issued by the National Cyber and Crypto Agency (BSSN) and SAFEnet, as well as academic publications relevant to the issues of defense economics and cyber security.

The data sources used in this study were derived from secondary data obtained from scientific literature, policy reports, and official government and non-government sources discussing economic, defense, and cyber aspects. The data was then selected, classified, and analyzed to obtain results relevant to the focus of the study. Data analysis used George C. Edwards III's Policy Implementation Theory as a theoretical basis. This theory has four main variables: communication, resources, disposition, and bureaucratic structure. To ensure data validity, this study uses source triangulation techniques by comparing various official documents, institutional reports, and academic literature. This aims to ensure the consistency and reliability of the information obtained. Through this approach, it is hoped that a comprehensive picture can be provided of the extent to which the implementation of defense economic policies strengthens national cyber capacity.

4. RESULT AND DISCUSSION

4.1 Implementation of Cyber Policy in Indonesia based on George C. Edward III's Theory

The implementation of cyber policy in Indonesia does not solely depend on the quality of the regulations created, but also on the harmony of the supporting elements in its implementation. In the realm of defense economics, this policy requires strong cross-sector synergy, readiness of implementers, and infrastructure that is responsive to increasingly developing digital threats. In order to evaluate the effectiveness of its implementation, George C. Edward II's theoretical framework is applied as an analytical instrument that focuses on the main factors that influence the success of policy implementation, namely communication, resources, disposition, and bureaucratic structure.

First, communication. Communication serves as a benchmark for assessing the extent to which a policy, particularly in the form of regulations, has been clearly communicated, uniformly interpreted, and consistently implemented by the officials responsible for its implementation. In the policy communication process, there are three main aspects to consider, namely transmission (how information is conveyed to the public), clarity of the information conveyed, and consistency (implementation of the communicated policy). Findings show that defense economic policies related to strengthening cyber capacity have been disseminated through various strategic documents, such as the issuance of Presidential Regulation No. 47 of 2023 concerning the National Cyber Security Strategy and Cyber Crisis Management as mandated by Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and the preparation of the National Cyber Security Action Plan for 2024-2028 and other derivative regulations related to digital transformation.

These documents serve as the main reference for all stakeholders in formulating and implementing national cyber policies, including aspects of investment, infrastructure development, and human resource capacity building. However, in practice, communication patterns between stakeholders are still not fully uniform and optimally coordinated. Differences in interpretation arise mainly in the areas of investment priorities, system security standards, and the division of roles in the development of national cyber capabilities. Each of the agencies involved has tasks and functions that are not always synchronized, so that when data leaks or cyber-attacks occur, the response is often fragmented and uncoordinated. This results in slow resolution and low accountability (Rosyadi & Sara, 2025).

The second is resources. Various supporting elements such as budget, human resources, and technology are necessary aspects in implementing policies in the cyber field. In terms of budget, Indonesia has begun to show its seriousness in facing cyber security challenges through the allocation of a special budget for cyber defense. These funds are used to form an incident response team and strengthen the national digital security infrastructure. According to Commission I of the Indonesian House of Representatives, the amount of budget provided is still relatively small compared to the growing and increasingly complex cyber threats. The budget for cybersecurity and cryptography programs experienced a significant increase in 2019 (Rp2,001.04 billion), then declined sharply in the following years and only reached Rp120.34 billion in 2023. See Figure 3.

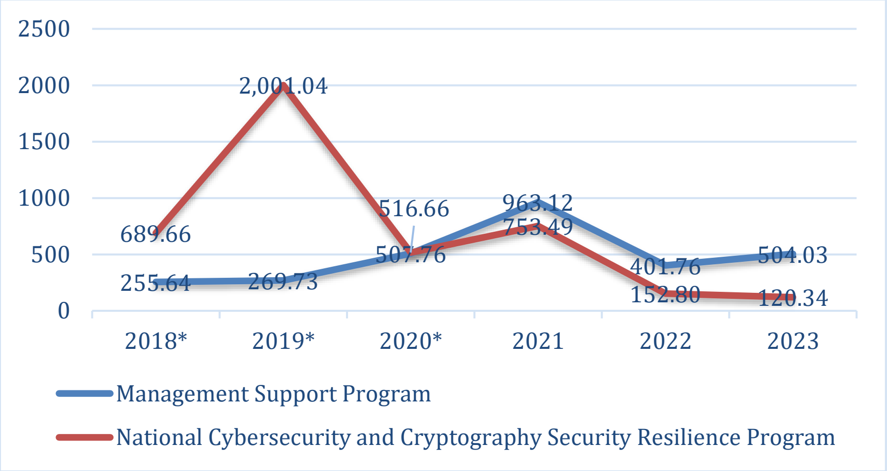

Figure 3. Budget Chart per Program at BSSN for 2018-2023 (in billions of rupiah)

Sources: Pusat Kajian Akuntabilitas Keuangan Negara, (2022)

In the field of human resources, Indonesia faces significant challenges in developing cybersecurity. According to data from the National Cyber Security Index (NCSI), Indonesia ranks 49th out of 176 countries in terms of cybersecurity with a score of 63.64 points based on data from 2016-2023. Among ASEAN member countries, Indonesia ranks 5th, behind Malaysia, Singapore, and Thailand, and equal to the Philippines (e-Governance Academy Foundation, 2023). These resource constraints hinder the establishment of an adequate framework and the training of experts who are urgently needed to deal with the increasing threats of cyber-attacks in various forms. Responding effectively to cyber threats requires personnel with in-depth technical competence in cybersecurity, digital forensic analysis skills, and practical skills in implementing appropriate response measures (Sarjito, 2023). In addition to the insufficient availability of human resources to meet the need for cyber experts, Indonesia's cybersecurity infrastructure is also often weak. This condition makes the government sector vulnerable to data breaches and information leaks.

The third is disposition. The attitude of policy implementers in defense and security agencies shows a high level of commitment to digitalization and strengthening cybersecurity, as evidenced by various capacity building and digital infrastructure modernization initiatives undertaken by BSSN and the Ministry of Defense in forming the TNI cyber unit. However, at the agency level, cyber issues are still often understood as purely technical matters, rather than strategic issues that determine national security and sustainability. This has resulted in the slow and uneven implementation of cybersecurity policies, especially in agencies that have not fully integrated cybersecurity into their strategic organizational agenda. Therefore, a paradigm shift from a technical approach to a strategic approach is needed, as well as increased inter-agency coordination so that cybersecurity can be fully integrated into the national defense and security agenda.

Fourth, bureaucratic structure. Handling cyber threats involves various ministries/institutions within the government. The ministries/institutions responsible for cyber defense in Indonesia include: (a) The National Cyber and Crypto Agency (BSSN) as the main institution that monitors, detects, and handles cyber threats nationally and coordinates with government and private agencies; (b) The Ministry of Defense (Kemhan) is responsible for national cyber defense, including the development of cyber defense strategies, oversight of strategic state assets, and coordination with the Indonesian National Armed Forces (TNI) and related agencies; (c) The Ministry of Communication and Digital Affairs (Komdigi) as the agency that manages digital infrastructure, oversees the digital space, and strengthens cybersecurity in the government and public sectors; (d) The Coordinating Ministry for Political and Security Affairs (Kemenko Polkam), which established the Cybersecurity and Data Protection Desk to strengthen coordination between ministries/agencies in maintaining cybersecurity and protecting personal data.

Although BSSN has been designated as the main authority, the involvement of various ministries and institutions in the field of cybersecurity has the potential to create bureaucratic complexity that can hinder the effectiveness of coordination and response to cyber incidents. Coordination between agencies such as Kominfo, BSSN, and Kemhan is still not optimal, resulting in delays in handling cyber incidents and a lack of information transparency. This is exacerbated by limited coordination mechanisms and bureaucratic obstacles that result in an inefficient response to cyber incidents (Ilaina & Nugraha, 2025).

4.2 The Impact of Cyber Policy on National Economic Resilience

Strengthening cyber security policy plays a strategic role in maintaining national economic resilience, especially as Indonesia's economic activities become increasingly integrated with digital systems. The link between cyber security and the economy is becoming ever closer, as disruptions to digital systems, whether in the form of cyber-attacks, data leaks, or attacks on critical infrastructure, have the potential to cause significant financial losses and disrupt the stability of strategic sectors. Global losses due to cybercrime are projected to surge from US$ 8.4 trillion in 2020 to US$ 23.8 trillion in 2027 (Hidayat, 2025). This situation confirms that cyber policy is not only a security instrument but also an important pillar in maintaining national economic sustainability.

Cyber policy has a direct impact on the stability of vital economic sectors. Disruption in these sectors can sever supply chains, hamper trade activities, and trigger market uncertainty. For example, attacks on energy or banking infrastructure can trigger a domino effect on industry, households, and even the state's fiscal sector. Therefore, strong cyber policies will help minimize potential vulnerabilities, increase system resilience, and strengthen public and business confidence in Indonesia's digital security.

On the other hand, cyber policy also has an impact on the efficiency and allocation of the defense budget. The implementation of coordinated policies can reduce post-incident recovery costs, reduce dependence on expensive foreign technology, and encourage the use of early detection technology that provides long-term efficiency. Conversely, weak or inconsistent policies can increase the fiscal burden on the state due to the costs of incident handling, equipment replacement, and recovery of affected systems. Thus, the quality of cyber policy has direct implications for the appropriate use of defense resources and the sustainability of the state budget.

4.3 Cyber Defense Policy Recommendations to Support National Resilience

In facing the increasing complexity of cyber threats that directly impact national stability, a strategic, adaptive, and cross-sector policy response is needed. Cyber threats are no longer merely a technical issue, but have become part of the dynamics of national defense, particularly in the context of non-military resilience. Therefore, the defense economy must be able to adjust its orientation to the needs of the digital era, placing cyber security as one of its top priorities. To address these challenges and strengthen national resilience as a whole, there are several policy recommendations that can be implemented, namely: (1) Strengthening Policy Communication Between Ministries/Institutions. Cooperation between ministries/institutions must be improved through uniform communication methods to reduce misunderstandings in policy implementation. Through good communication, the government can also encourage collaboration with the private sector and civil society to raise awareness of cyber threats that could disrupt economic stability; (2) Increased Investment in Human Resources and Technology. The government needs to develop human resources through education and training and strengthen the allocation of a special budget for cyber defense within the framework of the national defense economy. This includes technical cyber training for military and civilian personnel, the development of strategic digital infrastructure, and cyber-attack detection and mitigation systems. Cyber defense spending must be positioned as a long-term investment in non-military national security and economic independence in defense; (3) Simplification of the Bureaucratic Structure and National Cyber Management. Cyber defense policy requires a simpler, more transparent, and less overlapping bureaucratic structure. A comprehensive review of the division of authority between ministries/agencies is needed so that there is a uniform understanding of the policies implemented in accordance with their respective authorities.

5. CONCLUSION

Strengthening capacity in the cyber sector is a crucial element in the defense economy framework because current digital threats can directly affect economic stability and national security. Based on the application of George C Edward III's policy implementation theory, it can be seen that the main obstacles faced by Indonesia include communication between stakeholders that is not yet fully uniform and optimally coordinated, limited resources in terms of both budget and professional personnel, inconsistent commitment from implementers, and complex bureaucracy. These findings have an impact on the effectiveness of cyber defense policy implementation and efforts to maintain national economic resilience. This study recommends strengthening policy communication between institutions, developing human resources, and increasing technology investment through budget strengthening and simplifying the bureaucratic structure. This is expected to strengthen the cyber sector's preparedness in facing increasingly complex challenges to maintain economic resilience and national security.

Despite its contributions, this research still has opportunities for further exploration, particularly in deepening the understanding of cyber defense policies at the operational level. Due to the limitations of the secondary data used, future research is recommended to conduct analysis based on primary data through surveys or interviews with stakeholders. Furthermore, this study can also be developed through comparative studies with other countries to provide more comprehensive view.

Ethical Approval
Not Applicable

Informed Consent Statement
Not Apllicable

Authors' Contributions
NFAK contributed to the conceptualization of the study, formulation of research objectives, research design, development of the analytical framework using George C. Edward III's policy implementation model, literature study and document collection, data analysis and interpretation, and drafting the original manuscript. S contributed to the methodology refinement, validation of the analytical approach, critical review of policy and budget evidence, supervision throughout the research process, and reviewing and editing the manuscript. SI contributed to theoretical strengthening, synthesis of findings into policy implications, verification of interpretations and conclusions, and reviewing and editing the manuscript.

Disclosure Statement
The Authors declare that they have no conflict of interest

Data Availability Statement
The data presented in this study are available upon request from corresponding author for privacy

Funding
This study did not receive any external funding

Notes on Contributors

Nurul Faizah Al Khoiriyah
Nurul Faizah Al Khoiriyah is affiliated with Universitas Pertahanan Republik Indonesia

Suwito
Suwito is affiliated with Universitas Pertahanan Republik Indonesia

Sri Iswati
Sri Iswati is affiliated with Universitas Pertahanan Republik Indonesia

REFERENCES

Aditya, N. R., & Carina, J. (2025). TNI Punya Peran Baru Tangani Ancaman Siber, Apa Saja Tugasnya? *Kompas.Com*. https://nasional.kompas.com/read/2025/03/26/16292341/tni-punya-peran-baru-tangani-ancaman-siber-apa-saja-tugasnya

Ahmed, F. M., Molla, A. H., Uddin, R., & Chowdhury, T. R. (2023). *Advancing Cyber Resilience : Bridging the Divide Between Cyber Security and Cyber Defense*. *5*(6), 1–9.

Arce, D. (2023). Cybersecurity For Defense Economists. *Defense and Peace Economics*, *34*(6), 705–725. https://doi.org/10.1080/10242694.2022.2138122

e-Governance Academy Foundation. (2023). *National Cyber Security Index*. https://ncsi.ega.ee/country/id_2022/

Edward III, G. C. (1980). *Implementing Public Policy*. Congressional Quarterly Press.

Gaibulloev, K., Kollias, C., & Solomon, B. (2020). Defense and Peace Economics: The Third Decade in Retrospect. *Defense and Peace Economics*, *31*(4), 377–386. https://doi.org/10.1080/10242694.2020.1761221

Galinec, D. (2022). Cyber Security and Cyber Defense : Challenges and Building of Cyber Resilience Conceptual Model. *International Journal of Applied Sciences & Development*, *1*, 83–88. https://doi.org/10.37394/232029.2022.1.10

Hartley, K. (2020). Defense Economics. In *Cambrigde University Press*. Cambridge University Press. https://doi.org/10.1017/9781108887243

Hidayat, A. (2025). Ancaman Serangan Siber Bisa Bikin Rugi 397 Kuadriliun, Bank cs Harus Apa? *DetikFinance*. https://finance.detik.com/moneter/d-8205150/ancaman-serangan-siber-bisa-bikin-rugi-rp-397-kuadriliun-bank-cs-harus-apa

Ilaina, A. S. A., & Nugraha, I. F. (2025). Kesenjangan Kapabilitas Keamanan Siber Indonesia dalam Mitigasi Serangan Siber pada Layanan Publik Digital tahun 2020-2025. *Triwikrama: Jurnal Multidisiplin Ilmu Sosial*, *8*(6).

Kementerian Pertahanan RI. (2014). *Pedoman Pertahanan Siber*.

Kurhayadi. (2023). Public Policy Implementation: A Theoretical Review. *Ministrate Jurnal Birokrasi Dan Pemerintahan Daerah*, *5*(1), 10–18. https://doi.org/10.15575/jbpd.v5i1.23742

Ndubuisi, A. F. (2023). Strengthening national cybersecurity policies through coordinated threat intelligence sharing and real-time public-private collaboration frameworks. *International Journal of Science and Research Archive*, *8*(2), 812–831. https://doi.org/10.30574/ijsra.2023.8.2.0299

Pusat Kajian Akuntabilitas Keuangan Negara. (2022). *Urgensi Dukungan Anggaran dalam Keamanan Siber Indonesia*. www.pusatkajiankn.dpr.go.id

Rosyadi, S. Y., & Sara, R. (2025). The Urgency of Establishing a National Digital Commission to Ensure Responsive and Sustainable Cyber Governance in Indonesia. *Deposisi: Jurnal Publikasi Ilmu Hukum*, *3*(3), 62–71. https://doi.org/https://doi.org/10.59581/deposisi.v3i3.5441

SAFEnet. (2025). *Digital Rights Situation Report: Indonesia 2024*.

Saputro, G. E., & Prakoso, L. Y. (2021). Implementation of Economic Policies Facing Covid 19 in Supporting Nonmilitary Defense. *International Journal of Social Science and Human Research*, *04*(04), 634–642. https://doi.org/10.47191/ijsshr/v4-i4-11

Sarjito, A. (2023). Memikirkan Kembali Kebijakan Pertahanan di Era Peperangan Siber. *Publitas Jurnal of Social Sciences and Politics*, *10*(1), 75–91. https://doi.org/10.37858/publisitas.v10i1.330

Simorangkir, A., Sihombing, H., Sihite, P. I., & Parhusip, J. (2024). Ransomware pada Data PDN : Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber. *Jurnal Sains Student Research*, *2*(6), 324–331. https://doi.org/https://doi.org/10.61722/jssr.v2i6.2966

Sri, S. (2024). *Ekonomi Pertahanan Era Global: Kebijakan, Industri, dan Kerjasama Internasional*. CV. Aksara Global Akademia.

Susdarwono, E. T. (2020). A DESCRIPTION OF DEFENSE ECONOMY AS A SCIENCE. *Jurnal Utilitas*, *6*(1), 17–25. https://doi.org/10.22236/utilitas.v6i1.4784

Yanko, A., Hlushko, A., Onyshchenko, S., & Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. In *ECONOMIC AND CYBER SECURITY* (pp. 30–58). TECHNOLOGY CENTER PC. https://doi.org/10.15587/978-617-7319-98-5.ch2

Yusgiantoro, P. (2014). *Ekonomi Pertahanan*. PT Gramedia Pustaka Utama.