(Online) ISSN 2744-1741
Original Research

Defense and Security Studies
Vol. 5, No. 2, 2024, pp. 74-83
https://doi.org/10.37868/dss.v5.id272

Formation of the TNI cyber force: A strategic and policy analysis

Aris Sarjito[1*]
[1] Faculty of Defense Management, Republic of Indonesia Defense University, Indonesia

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

Received: Oct. 13, 2024
Revised: Nov. 13, 2024
Accepted: Nov. 15, 2024
Online: Nov. 20, 2024

Abstract

The increasing cyber threats in Indonesia require strengthening the country's defense strategy. This study focuses on the formation of the Indonesian National Army (TNI) Cyber Force as part of efforts to strengthen the country's cyber security in facing increasingly complex threats. The purpose of this study is to analyze the policy and strategy for the formation of the TNI Cyber Force and evaluate the synergy between institutions, especially with the National Cyber and Crypto Agency (BSSN). This study uses a qualitative method with a secondary data analysis approach, including reports from Fortinet, AwanPintar.id, and national policy documents related to cybersecurity. The research findings show that the TNI CyberForce has a crucial role in protecting Indonesia's critical infrastructure from the threat of botnets, ransomware, and other cyber-attacks. The synergy between the TNI and BSSN is key to building an effective cyber defense system. Although there hasbeen an increase in cyber readiness, this study found that challenges still exist, including in terms of human resources and the technology used. In conclusion, theformation of the TNI Cyber Force is an important step in dealing with cyber threats,but there needs to be further strengthening in cross-sector coordination and adoption of the latest technology.

Keywords: BSSN; cyber security; national defense; synergy between institutions;TNI Cyber Force

1. Introduction

Research on the formation of the Indonesian National Army (TNI) Cyber Force is rooted in the growing global cyber security threats, which have become a primary focus in modern defense strategies. The rapid development of information and communication technology has created a new dimension in warfare—cyber warfare— requiring the military to adopt more responsive strategic measures. According to White [1], cyberattacks have increased in both volume and severity, prompting many countries, including Indonesia, to integrate cyber defense into their military structures.

At the international level, countries like the United States and Russia have pioneered the establishment of specialized military units dedicated to cyber defense [2]. This has inspired Indonesia to take similar steps with the formation of the TNI Cyber Force, aimed at securing the nation's digital sovereignty from external threats. Recent research by Mahendra [3] suggests that Indonesia is currently at a critical juncture in strengthening its cyber security policies through military structural reforms, particularly by integrating cyber defense strategies into national policies.

Indonesia has faced a significant rise in the number of cyberattacks in recent years. According to reports from Fortinet [4] and AwanPintar.id [5], cyberattacks in Indonesia have been increasing in both quantity and complexity. Local companies and critical infrastructure have been the main targets of various types of attacks, including ransomware, botnets, and vulnerability exploits. This data underscores the importance of proactive measures and robust policies to strengthen Indonesia's cyber defense systems.

The following Table 1 presents key data from these reports.

Table 1. Cyberattack Data in Indonesia (2021-2024) [6,7,8,9]

Category	2021	2022	2023	2024 (H1)
Number of cyberattacks	320,000,000	347,172,666	500,000,000	2,499,486,085
Dominant type of attack	Ransomware	Ransomware	Ransomware	Admin access takeover
Botnet duration (days)	7	10	83	83
Botnet attacks	19,104,200	35,911,749	35,911,749	126% increase
Ransomware attacks	Decreased 13%	Decreased 13%	Decreased 13%	-
Detected viruses in Indonesia	JS/Agent.CY!tr (4.8%)	MSOffice CVE_2018_0798 (2.5%)	-	-
Cyber Security Score (NCSI)	38.96 (rank 83)	63.64 (rank 49)	-	-

The data above shows that the number of cyberattacks in Indonesia surged drastically, from 320 million in 2021 to more than 2.4 billion in the first half of 2024 alone. The most dominant attacks in recent years have been ransomware, though its detection has decreased by 13% over the past five years. However, the more concerning type of attack in 2024 is the takeover of admin access, indicating an increase in hackers' ability to control victims' systems.

The rise in botnet duration from 7 days in 2021 to 83 days in 2023-2024 indicates that botnets are becoming more persistent and harder to detect. Another important finding is the significant increase in malware variants and vulnerability exploits, especially viruses like JS/Agent.CY!tr and vulnerabilities in MSOffice CVE_2018_0798.

Indonesia's Cyber Security Score also improved, from 38.96 in 2022 to 63.64 in 2023, demonstrating an enhancement in national cyber readiness. However, many challenges remain, particularly regarding the surge of attacks originating domestically, as found by AwanPintar [5], with most attacks coming from the Jakarta and Depok areas.

These findings highlight the urgency for both the government and private sectors to take proactive steps in protecting Indonesia's digital infrastructure, given the increasing risks of more targeted and sophisticated attacks.

The formation of the TNI Cyber Force, as outlined by Arianto & Anggraini [10], is also a response to the rising domestic cyber security threats, with hacking incidents against critical infrastructure such as energy and transportation spiking sharply. This study shows that the Cyber Force will function not only as a protector of digital infrastructure but also as a diplomatic instrument in addressing escalating international cyber conflicts [11].

Therefore, this research explores the strategies and policies behind the formation of the TNI Cyber Force, as well as how the TNI can position itself to address global cyber challenges. The focus of this study is to understand the policy dynamics implemented by Indonesia's Ministry of Defense and the TNI in developing cyber capacity and to analyze the relevance and effectiveness of the adopted cyber defense strategies.

The empirical problem in this study concerns the implementation of strategies and policies in forming the TNI Cyber Force in Indonesia. Although the TNI has established a cyber unit, there is no comprehensive data on the operational effectiveness of the Cyber Force in addressing real cyber threats. Hacking incidents targeting critical national infrastructure, such as the transportation system and energy sector in recent years, indicate that Indonesia's cyber defense efforts still have significant weaknesses [10]. Additionally, challenges such as limited human resources with technical expertise in cybersecurity and lack of coordination between institutions in responding to cyberattacks reveal a gap between the designed policies and actual implementation [12].

Normatively, the issues arising from the formation of the TNI Cyber Force not only touch on national security aspects but also relate to broader ethical and legal issues. The use of cyber forces within a military context raises questions about the boundaries of technology use in cyber warfare, particularly concerning human rights and digital sovereignty. The regulations and legal frameworks underpinning the TNI Cyber Force must address these questions while balancing national security with individual freedoms in the digital realm.

Below are several national and international regulations that serve as the legal framework for the formation of the TNI Cyber Force:

- Law no. 3 of 2002 on state defense [13]

  Article 1, paragraph (1) defines state defense as efforts to maintain the sovereignty of the country, territorial integrity, and the safety of the nation from threats, including cyber threats. This law serves as the primary legal basis for the formation of the TNI, including the development of the Cyber Force to protect Indonesia's digital sovereignty. In the context of increasing cyber threats, the TNI must expand its operational scope to cyberspace in accordance with its national defense mandate.

- Law no. 34 of 2004 on the Indonesian National Armed Forces (TNI) [14]

  Article 7, paragraph (2) explains the TNI’s main tasks in maintaining the integrity of the Republic of Indonesia, including through military operations other than war (MOOTW), which can encompass cyber defense. This law mandates the TNI to engage in unconventional military operations, such as cyber warfare, to protect the nation's strategic assets in cyberspace.

- Presidential regulation no. 82 of 2022 on the National Cyber and Encryption Agency (BSSN) [15]

  Articles 2 and 3 outline BSSN’s authority in maintaining information and cyber security and its cooperation with other institutions, including the TNI, to protect critical infrastructure. BSSN is a key partner in the formation and operation of the TNI Cyber Force, requiring close coordination between the two agencies to holistically address cyber threats.

- The Geneva conventions and additional protocols (1949 and 1977) [16]

  Although the Geneva Conventions do not explicitly regulate cyber warfare, the principles regarding the protection of civilians and critical infrastructure during armed conflicts also apply in the context of cyber warfare. The TNI Cyber Force must operate within an international legal framework that upholds civil protection rights, especially regarding cyberattacks that could impact civilian infrastructure such as power grids or communication systems.

- Tallinn manual on the international law applicable to cyber warfare (Tallinn Manual 2.0) [17]

  This manual explains the application of international law, including the laws of war, in the context of cyberattacks. The Tallinn Manual provides guidelines on how cyber operations can be conducted by states during conflict, including by military forces. The TNI Cyber Force must ensure that its operations stay within the bounds of international law, particularly regarding acts of cyber aggression.

- Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) [18]

Articles 29 through 31 regulate information security, prohibitions against illegal access, and electronic data protection. The TNI Cyber Force must also comply with the ITE Law, especially concerning the use of cyber technology in a military context that may involve accessing sensitive or electronic data.

In forming the TNI Cyber Force, there must be alignment between national and international legal frameworks to ensure that all forms of cyber operations are conducted in accordance with applicable legal principles. While national defense remains a priority, transparency, accountability, and the protection of human rights in the digital world must always be upheld. These regulations form the foundation for determining the operational boundaries of the TNI Cyber Force and ensuring that its military activities do not violate international legal principles or civil rights in cyberspace.

2. Research method

To ensure reproducibility, this research on "The Formation of the TNI Cyber Force: A Strategic and Policy Analysis" adopts a qualitative research method using secondary data, following the approach outlined by Creswell [19]. Specifically, content analysis was employed, as described by Krippendorff [20], to systematically analyze the selected data sources, focusing on policy documents, cybersecurity reports, and relevant regulations, including the Defense Law, the TNI Law, and global cybersecurity threat reports from Fortinet [4] and the National Cyber and Encryption Agency (BSSN).

Content analysis was conducted to identify key themes related to cybersecurity strategies, such as the effectiveness of collaboration between the TNI and BSSN and the challenges encountered in implementing cyber defense policies. The analysis followed a structured coding process based on pre-defined categories that align with cybersecurity policy and strategy evaluation frameworks.

The use of secondary data is central to this study due to the availability of comprehensive policy documents, legal regulations, and national and international cybersecurity reports. Key sources include the Fortinet [4] Global Threat Report, BSSN's cybersecurity policy documents, and relevant Indonesian cybersecurity regulations. These sources provide detailed insights into the formulation and implementation of policies in response to evolving cyber threats.

To ensure that findings were reliable and valid, content analysis was conducted in stages. First, a thorough review of documents was performed, followed by open coding to identify recurring themes. This was followed by axial coding to group-related themes, enabling a more focused analysis of challenges and successes in the TNI's formation of the Cyber Force. Modifications of Krippendorff [20] method included a case study approach to assess specific incidents of cyberattacks on Indonesia's critical infrastructure. This case study method allowed for the exploration of strategic and policy implications in real-world contexts.

3. Results and discussion

3.1 Research findings

This study found that the formation of the TNI Cyber Force is a response to the increasing complexity of cyber threats in Indonesia and globally. According to data from Fortinet [4], Indonesia experienced over 35 million botnet attacks in the first quarter of 2023, with a significant increase in attack duration, reaching up to 83 days. Botnets like Ghost Rat and Mirai were frequently used for Distributed Denial of Service (DDoS) attacks and data theft. These findings highlight the importance of strengthening the military's cyber units to protect the country's critical infrastructure.

Additionally, data from AwanPintar.id [5] indicates that the number of cyberattacks in Indonesia during the first half of 2024 reached 2.4 billion, a drastic increase compared to 347 million attacks in the same period the previous year. This further emphasizes the need for the establishment of the TNI Cyber Force as part of the national defense strategy to counter these threats.

In terms of policy, Presidential Regulation No. 82 of 2022 on the National Cyber and Encryption Agency (BSSN) regulates the coordination between BSSN and the TNI in the protection of cyber infrastructure. This research found that synergy between BSSN and the TNI Cyber Force is crucial in addressing the growing challenges in cybersecurity. As highlighted by Chotimah [12], closer collaboration between these agencies will enhance the effectiveness of national cyber defense, especially in anticipating both domestic and international cyber threats.

Regarding international law, the implementation of the Tallinn Manual 2.0 provides guidelines on how military cyber operations must comply with the laws of war. The TNI Cyber Force needs to ensure that its operations remain within the boundaries of international law, especially concerning attacks that may impact civilian infrastructure.

White [1] also underscores the importance of coordination between the military and civilian sectors in safeguarding a nation's digital sovereignty, as cyber threats can easily target vital civilian sectors.

The research also revealed that Indonesia ranks 49th globally in the National Cybersecurity Index (NCSI) 2023, with a score of 63.64. Although this ranking has improved from 83rd place in 2022, Indonesia still needs to increase its cybersecurity readiness, particularly as attacks on critical infrastructure, such as the National Data Center (PDN), have been rising, with a ransomware attack by LockBit 3.0 occurring in mid-2024 [9].

This study uncovers several critical facts regarding the formation of the TNI Cyber Force and the cybersecurity challenges faced by Indonesia. The following Table 2 summarizes the key findings:

Table 2. Key Research Findings on the Formation of the TNI Cyber Force

Category	Data	Source
Number of Botnet Attacks in Indonesia (Q1 2023)	35,911,749 attacks, with Ghost Rat leading (19.87% growth)	Fortinet [4]
Botnet Duration	Botnet duration increased to 83 days (2023), 1,000x longer than in previous years	Fortinet [4]
Number of Cyberattacks in Indonesia (H1 2024)	2.4 billion attacks (up from 347 million attacks in the same period the previous year)	AwanPintar.id [5]
BSSN and TNI Coordination	Synergy between BSSN and the TNI Cyber Force is needed to protect national cyber infrastructure	Presidential Regulation No. 82 of 2022 [21]
Indonesia’s Cybersecurity Ranking	Indonesia ranked 49th globally in the NCSI 2023 with a score of 63.64	NCSI [22]
Ransomware Attack on PDN	LockBit 3.0 ransomware attack targeted the National Data Center in mid-2024	tirto.id [9]
International Law on Cyber Warfare	TNI Cyber Force operations must comply with international law, as outlined in the Tallinn Manual 2.0	White [1]

(Sources: Fortinet [4]; AwanPintar.id [5]; Presidential Regulation No. 82 of 2022 [21]; NCSI [22]; tirto.id [9], White [1].)

The table shows that the significant number of cyberattacks in Indonesia, particularly botnet and ransomware attacks, underscores the urgency of forming the TNI Cyber Force. Data from Fortinet (2023) highlights the sharp increase in botnet attack duration, leaving Indonesia's digital infrastructure vulnerable for extended periods. Moreover, with over 2.4 billion cyberattacks in the first half of 2024 [5], the creation of a military cyber unit becomes a strategic step in tackling these massive threats.

Coordination between BSSN and the TNI Cyber Force is crucial to ensure the protection of national cyber infrastructure, as stipulated by Presidential Regulation No. 82 of 2022. One of the challenges includes ensuring that the TNI operates within the framework of international law, as explained in the Tallinn Manual 2.0 [23].

Despite Indonesia’s significant improvement in cybersecurity rankings, rising from 83rd place in 2022 to 49th place in the NCSI 2023, more intensive efforts are required to reach a higher level of cyber readiness. The ransomware attack on the National Data Center (PDN) also highlights the need to bolster the security of strategic data, particularly in government institutions [9].

These findings confirm that the TNI Cyber Force is not only a crucial instrument in national defense but also requires cross-sector synergy and adherence to international law in conducting cyber operations.

3.2 Interpretation of research findings

The findings of this research reveal the importance of establishing the TNI Cyber Force as part of a national defense strategy that is responsive to the increasing cyber threats in Indonesia. The sharp rise in cyberattacks, particularly botnet and ransomware attacks, indicates significant vulnerabilities to the country's critical infrastructure. The data presented shows that more than 35 million botnet attacks were recorded in the first quarter of 2023, with botnet attack durations increasing to 83 days. This illustrates that cyber threats are becoming more persistent and require stronger and better-coordinated defense measures.

The surge in cyberattacks from 347 million in the first half of 2023 to 2.4 billion in the first half of 2024 represents a substantial increase, highlighting how rapidly these threats are evolving. This underscores the urgent need for the TNI, through the Cyber Force, to play a more active role in safeguarding the nation’s digital infrastructure. The coordination between BSSN and the TNI Cyber Force, as regulated by Presidential Regulation No. 82 of 2022, is critical to ensuring that both institutions can effectively address dynamic and targeted cyber threats.

Although Indonesia has improved its cybersecurity score, rising from 83rd place in 2022 to 49th place in 2023 on the National Cybersecurity Index (NCSI), the continuing rise of cyber threats emphasizes that efforts to strengthen cyber defense must be accelerated. This improvement in the score indicates progress in national cyber readiness, yet there remain gaps that must be addressed, especially in securing strategic government infrastructure, as seen from the ransomware attack on the National Data Center (PDN) in 2024.

In an international context, the operations of the TNI Cyber Force must remain within the boundaries of international law governing the use of cyber force, as outlined in the Tallinn Manual 2.0. This means that any military actions conducted by the TNI's cyber unit, particularly regarding cyber aggression, must comply with the laws of war and protect civil rights as well as critical infrastructure that may be impacted.

Overall, these findings indicate that the TNI Cyber Force has the potential to become a key instrument in addressing the growing cyber threats in Indonesia. However, institutional strengthening, cross-sector coordination, and compliance with both national and international regulations are necessary for it to function optimally in protecting the country’s digital sovereignty.

3.3 Comparison with literature

The findings of this research show that the formation of the TNI Cyber Force aligns with global trends in which countries are increasingly strengthening their cyber defenses as part of their national security strategies. Research by Hatch [2] indicates that countries such as the United States and Russia have long-established military cyber units to address the continuously evolving cyber threats. Similarly, the establishment of the TNI Cyber Force reflects Indonesia's need to adapt to new defense dynamics, particularly with the growing complexity of threats like botnets and ransomware. This finding is supported by the Fortinet report [4], which recorded a surge in botnet attack durations of up to 83 days, highlighting that these threats are becoming more persistent and difficult to manage with conventional defense approaches.

Additionally, Sarjito [24] emphasizes the importance of collaboration between military and civilian agencies to enhance the effectiveness of cyber defense. In the context of Indonesia, the synergy between BSSN and the TNI Cyber Force, as regulated by Presidential Regulation No. 82 of 2022, is crucial. This research is consistent with the literature that stresses cross-institutional cooperation as a key element in building resilient cyber defense. This is further reinforced by White's study [1], which underscores the need for coordination between civilian and military sectors in facing cyber threats that are global and interconnected.

From an international legal perspective, the research findings also align with the principles outlined in the Tallinn Manual 2.0. As explained in the manual, cyber operations conducted by the military must comply with international law, including the laws of war, to ensure that any cyber actions taken do not violate human rights or target critical civilian infrastructure. These findings are consistent with the arguments in the literature, which assert that legal boundaries in cyber operations are essential to maintaining the legitimacy of military actions in cyberspace.

The comparison between these findings and the existing literature demonstrates that Indonesia is following the global trend of strengthening national cyber defenses. However, the literature also highlights that Indonesia still needs to enhance its cyber capabilities and infrastructure, as reflected by the significant rise in cyberattacks in 2024. While AwanPintar.id [5] reported a surge in cyberattacks reaching 2.4 billion in the first half of 2024, comparisons with other countries reveal that Indonesia's cyber readiness, though improving, still lags behind some neighboring Southeast Asian nations such as Malaysia and Singapore, which rank higher in the National Cybersecurity Index (NCSI).

Thus, the findings of this research are consistent with the existing literature but also highlight the need for more intensive policy reinforcement, strategic planning, and institutional synergy to ensure that the TNI Cyber Force can effectively address the ever-evolving cyber threats.

3.4 Theoretical implications

This research reinforces the importance of integrating cyber capabilities into military defense, in line with the concept of cyber warfare, which is increasingly recognized as a key component of modern national security [2]. Additionally, the theory of collective security, which involves cross-agency synergy, is highly relevant, as demonstrated by the coordination between the TNI Cyber Force and the National Cyber and Encryption Agency (BSSN) in addressing rapidly evolving cyber threats [1]. This supports the idea that cybersecurity requires both national and international collaboration, as outlined in the Tallinn Manual 2.0 on the regulation of cyber operations by states [23].

The formation of the TNI Cyber Force also strengthens the theory of defense systems, where cyberspace is considered an essential component of a nation's broader defense system, which must be integrated with air, land, and sea forces [3].

3.5 Practical implications

This research provides several significant practical implications related to the formation of the TNI Cyber Force in addressing increasingly complex cyber threats.

First, the findings emphasize the importance of enhancing human resource capacity in cyber defense. The TNI Cyber Force requires personnel who are specially trained to manage cyber threats, including the ability to detect, respond to, and mitigate technical and targeted attacks. Investment in cybersecurity training and certification for military personnel is a crucial step toward strengthening national cyber resilience.

Second, the synergy between the National Cyber and Encryption Agency (BSSN) and the TNI Cyber Force must be reinforced through improved coordination and information sharing regarding cyber threats. The research indicates that inter-agency cooperation is essential to create a more holistic and integrated cyber defense system. This could be achieved by establishing clear cooperation protocols and a shared platform for real-time threat data exchange between BSSN and the TNI.

Third, the TNI Cyber Force needs to implement advanced cybersecurity technologies and infrastructure, including artificial intelligence (AI)-based technology to quickly detect evolving threats, as identified in the Fortinet report [4]. The use of AI and machine learning technologies in monitoring cyber threats can enhance response speed to attacks and help prioritize vulnerability patching in defense systems.

Fourth, the TNI Cyber Force should strengthen international relations and expand participation in global forums discussing cybersecurity, as recommended by the Tallinn Manual 2.0. This is necessary to ensure that cyber operations comply with international law and to gain access to relevant global cyber intelligence. Active participation in international cooperation will enable Indonesia to better protect its strategic infrastructure from global-scale attacks.

Fifth, the formation of the TNI Cyber Force lays the foundation for raising cybersecurity awareness across government institutions and the private sector. The research shows that with the growing number of cyberattacks, it is vital for the government to prioritize cybersecurity not only in the military sector but also in other critical sectors such as energy, transportation, and finance. Implementing policies that emphasize preventive cybersecurity measures across all layers will strengthen overall national digital security.

Thus, the practical implications of this research include enhancing personnel training, inter-agency cooperation, adopting cutting-edge technologies, fostering international collaboration, and spreading cybersecurity awareness nationwide.

3.6 Research limitations and future research

This study has several limitations that should be noted.

First, it relies primarily on secondary data, which means it does not include direct interviews with policymakers or military personnel involved in the formation of the TNI Cyber Force. This limits the depth of understanding regarding the internal processes related to the establishment and operationalization of the Cyber Force. More in-depth information obtained through direct interviews or field observations could provide a more comprehensive picture of the institutional dynamics and challenges faced by the TNI Cyber Force.

Second, the research focuses on national policy and does not thoroughly examine how international cybersecurity policies influence the strategies of the TNI Cyber Force. Given that cybersecurity issues are cross-border in nature and heavily influenced by global dynamics, this limitation results in an analysis that lacks consideration of the direct impact of international legal frameworks and cybersecurity strategies on domestic policy.

Third, the study is more focused on the strategic and policy aspects, with limited emphasis on the technical aspects of the TNI Cyber Force's formation, such as the technological infrastructure and cyber operational systems utilized. Further technical exploration into the technologies adopted by the Cyber Force, such as the use of artificial intelligence, cybersecurity systems, and protocols employed to counter cyberattacks, would provide deeper insights into the operational readiness of the TNI's cyber unit.

Based on the limitations mentioned above, future research can focus on several key areas.

First, field research using qualitative methods, involving in-depth interviews with military policymakers and cybersecurity experts, could provide sharper insights into the formation and operationalization of the TNI Cyber Force. This research could also include perspectives from the private sector that collaborates with the TNI to strengthen national cybersecurity.

Second, international comparative research could be conducted to compare military cybersecurity strategies in Indonesia with other countries that are more advanced in developing military cyber units, such as the United States, Russia, and China. This would help identify best practices that Indonesia could adopt to strengthen its cyber defense.

Third, future research could also focus on the technical aspects of cyber defense, such as the technologies used in detecting and responding to cyber threats. This could include studies on the effectiveness of artificial intelligence (AI) and machine learning in managing cyber threats in the military domain.

Fourth, further studies on the international legal framework related to cyber warfare and Indonesia’s involvement in global cybersecurity forums could also be an important direction for future research. This research could explore how international regulations influence the operations of the TNI Cyber Force and to what extent Indonesia complies with global norms in conducting military cyber operations.

By addressing these limitations and exploring broader and deeper research areas, future studies can contribute more comprehensively to understanding the role and effectiveness of the TNI Cyber Force in tackling cyber challenges in the modern era.

4. Conclusions

This study emphasizes the critical role of the TNI Cyber Force in responding to the growing complexity and volume of cyber threats in Indonesia. The rise in cyberattacks, particularly botnet and ransomware incidents, highlights the urgent need for a dedicated military cyber unit to enhance national cybersecurity, protect vital infrastructure, and maintain digital sovereignty. The significant increase in attacks, as indicated by data from Fortinet [4] and AwanPintar.id (2024) [5], underscores this necessity.

The collaboration between the TNI Cyber Force and the National Cyber and Encryption Agency (BSSN), as mandated by Presidential Regulation No. 82 of 2022, is essential for effectively countering cross-border and dynamic cyber threats. Furthermore, ensuring compliance with international laws, such as those detailed in the Tallinn Manual 2.0, is vital for maintaining the legitimacy of TNI's cyber operations within the global legal framework.

While Indonesia has made progress in improving its cybersecurity, as evidenced by its rising rank in the 2023 National Cybersecurity Index (NCSI), significant challenges remain. These include the need for enhanced human resources, the adoption of advanced technologies, and increased international cooperation to further strengthen the nation's cyber defense capabilities.

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.

Declaration of use of AI in the writing process

The author used ChatGPT during the preparation of this work to assist with language editing and refining the manuscript structure. The author reviewed and edited the work as necessary and took full responsibility for the final version.

References

[1] J. White, "Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies.," *Global Security Studies*, vol. 7, no. 4, 2016.

[2] B. Hatch, "The future of strategic information and cyber-enabled information operations," *Journal of Strategic Security*, vol. 12, no. 4, pp. 69–89, 2019.

[3] Y. C. Mahendra, N. K. D. S. A. Pinatih, "Cyber Security Handling Strategy in Indonesia," *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, vol. 6, no. 4, pp. 1941–1949, 2023.

[4] Fortinet, "Global Threat Landscape Report A Semiannual Report by FortiGuard Labs," 2023. Accessed: Oct. 13, 2024. [Online]. Available from: https://www.fortinet.com/content/dam/fortinet/assets/threat- reports/threat-report-1h-2023.pdf

[5] AwanPintarid, "AwanPintar.id | Indonesia Alert - Digital Threat Report in Indonesia Semester 1 of 2024," 2024. Accessed: Oct. 13, 2024. [Online]. Available from: https://www.awanpintar.id/wp-content/uploads/2024/08/2024_AwanPntar.id_Laporan_Ancaman_Digital_sem1_2024_Green.pdf

[6] CSIRT BAIS TNI, "Global Threat Report 2023: Cybersecurity and Trends in Indonesia," CSIRT BAIS TNI. Accessed: Oct. 12, 2024. [Online]. Available: https://csirt.bais-tni.mil.id/posts/laporan-ancaman-global-2023-keamanan-siber-dan-tren-di-indonesia

[7] KumparanTECH, "Cyber Attacks on Indonesia Increase 6 Times in H1 2024, Majority from Domestic,"kumparanTECH. Accessed: Oct. 12, 2024. [Online]. Available from : https://kumparan.com/kumparantech/serangan-siber-ke-ri-naik-6-kali-lipat-pada-h1-2024-mayoritas- dari-dalam-negeri-23PnYQpafrf/4.

[8] Tempo.co, “BSSN: 361 million Cyber Attacks to Indonesia,” tempo.co. Accessed: Oct. 12, 2024. [Online]. Available from: https://bisnis.tempo.co/read/1797613/bssn-361-juta-serangan-siber-ke-indonesia

[9] Tirto.id, “What is the Cybersecurity Score and Rating in Indonesia?,” tirto.id. Accessed: Oct. 12, 2024. [Online]. Available from: https://tirto.id/berapa-skor-dan-peringkat-keamanan-siber-di-indonesia-gZ1s

[10] A. R. Arianto, G. Anggraini, “Building Indonesia's national cyber defense and security to deal with global cyber threats through the Indonesia security incident response team on internet infrastructure (ID-SIRTII),” *Jurnal Pertahanan dan Bela Negara*, vol. 9, no. 1, pp. 13–30, 2019.

[11] A. S. Waskita, H. Sidik, “Indonesia's Cyber Diplomacy in the Implementation of Capacity Building on National Cybersecurity Strategy Workshop 2019,” *Padjadjaran Journal of International Relations*, vol.5, no. 2, p. 142, 2023.

[12] H. C. Chotimah, “Cyber Security Governance and Cyber Diplomacy in Indonesia under the Institution of the State Cyber and Cryptography Agency [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency],” *Jurnal Politica Dinamika Masalah Politik Dalam Negeri danHubungan Internasional*, vol. 10, no. 2, pp. 113–128, 2019.

[13] A. F. Lubis, “Implementation of Law Number 3 of 2002 concerning State Defense in Dealing with military Disturbances,” *Jurnal Begawan Hukum (JBH)*, vol. 2, no. 1, pp. 310–319, 2024.

[14] DataIndonesia.id, “Law No. 34 of 2004 concerning the Indonesian National Army,” DataIndonesia.id. Accessed: Oct. 13, 2024. [Online]. Available: https://dataindonesia.id/regulasi/detail/uu-no-34-tahun- 2004-tentang-tentara-nasional-indonesia

[15] M. Rizki, “Development of Indonesia's Defense/Cyber Security System in Facing the Challenges of Technological and Information Development,” *Politeia: Jurnal Ilmu Politik*, vol. 14, no. 1, pp. 54–62, 2022.

[16] M. Bothe, K. J. Partsch, W. A. Solf, *New rules for victims of armed conflicts: commentary on the two 1977 protocols additional to the Geneva Conventions of 1949*. Martinus Nijhoff Publishers, 1982.

[17] M. N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, vol. 141. Cambridge University Press, 2013.

[18] L. H. Sujamawardi, “Juridical Analysis of Article 27 paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions," *Dialogia Iuridica*, vol. 9, no. 2, 2018.

[19] J. W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications, 2014.

[20] K. Krippendorff, Content analysis: An introduction to its methodology. Sage Publications, 2018.

[21] JDIH, “Peraturan Presiden Nomor 82 Tahun 2022 tentang Badan Siber dan Sandi Negara (BSSN).,” JDIH. Accessed: Oct. 13, 2024. [Online]. Available: https://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021#:~:text=Perpres%20ini%20mengatur%20mengenai%20kedudukan%2C%20tugas%2C%20dan%20fungsi,bertanggung%20jawab%20kepada%20Presiden%20yang%20dipimpin%20oleh%20Kepala.

[22] NCSI, “NCSI Rankings 2023,” e-Governance Academy Foundation. Accessed: Oct. 13, 2024. [Online]. Available: https://ncsi.ega.ee/ncsi-index/

[23] E. T. Jensen, “The Tallinn Manual 2.0: Highlights and Insights,” *Geo. J. Int’l L.*, vol. 48, p. 735, 2016.

[24] A. Sarjito, “National Defense Ecosystem Model Based on Collaboration Between Government, Industry and Society,” *JISIP UNJA (Jurnal Ilmu Sosial Ilmu Politik Universitas Jambi)*, pp. 32–44, 2024