The Indonesian Journal of Development Planning
July 2026, Vol 10, No. 2, 197 - 213
https://doi.org/10.36574/jpp.v10i2.787

Research Article

Improving The Capacity of Human Resources in Cybersecurity to Support Defense Diplomacy in The Digital Era

Alia Noorayu Laksono[1], Editha Praditya Duarte[2], Yermia Hendarwoto[3]

[1, 2, 3] Republic of Indonesia Defense University

Abstract

This study aims to analyze the efforts and effectiveness of enhancing Human Resources (HR) capacity in Indonesian cybersecurity during the 2020–2024 period, in response to the surge and complexity of cyber threats. Based on data from the National Cyber and Crypto Agency (BSSN), the number of cyber incidents has continued to rise sharply, a situation closely linked to the availability of competent cybersecurity human resources. The research method used is qualitative analysis and data from various literature reviews. The results indicate that although there are existing plans for Human Resources (HR) capacity development, the quantity of trained cybersecurity HR remains low, especially in advanced specialization fields such as threat intelligence, forensics, and cloud security. Furthermore, cybersecurity technologies often lag behind the latest technological advancements and emerging types of threats. The main recommendations of this study include increasing national cybersecurity HR capacity and enhancing sustainable and structured collaboration among BSSN, the Indonesian House of Representatives (DPR RI), Industry, and the cyber community to strengthen national cyber resilience.

Article History:
Received: 7 April, 2026
Accepted: 21 June, 2026
Published: 30 July, 2026

Keywords:
cybersecurity; human resources; cyber threats; National Cyber Resilience.

Correspondence Email:
noorayulaksono@gmail.com

1. Introduction

Digital transformation has brought fundamental changes to the spectrum of threats faced by countries, particularly in the field of defense. Cyber threats can no longer be understood solely as technical disruptions to information systems, but have evolved into strategic instruments that have the potential to affect political, economic, and national security stability across borders. In this development, cyberspace has not only emerged as a new domain of defense, but also as an arena for diplomacy, where a country's actual capabilities are an important factor in building legitimacy and trust at the international level.

Indonesia's cybersecurity occupies a highly strategic and important position in today's digital era. Cybersecurity directly impacts national security, the economy, and the lives of society. The dimensions of cybersecurity include efforts to protect national critical infrastructure, safeguard digital sovereignty, and support digital transformation for economic growth. One of the most crucial components in establishing cybersecurity is the human resource (HR) factor, which must be continuously enhanced. The development of Indonesia's cyber workforce is a strategic focus mandated by law and entrusted to the National Cyber and Crypto Agency (BSSN) as a critical effort to face increasingly complex cyber threats.

The development of national cyber resilience does not depend solely on technological sophistication but fundamentally relies on the availability of competent digital talent. As emphasized in national development planning, the cyber talent gap remains a major obstacle to achieving the 2025 digital economy targets (Bappenas, 2023). The

problem of human resources in Indonesia's cybersecurity sector lies in the low quantity and quality of cyber experts and limited mastery of modern technology. In addition, low public awareness of cybersecurity across different levels of society continues to be a vulnerability that must be anticipated amid rapid digital transformation and the escalation of complex cyber threats.

The issue of cybersecurity has shifted from a purely technical problem to a national security concern that has been securitized — transforming from a technical issue into an existential threat. This securitization process legitimizes government institutions (such as BSSN) to allocate resources and formulate cybersecurity defense policies, including programs that accelerate the capacity-building of cyber human resources (Buzan, Waever, & Wilde, 1998). Referring to the available data, cyber threats targeting Indonesia indicate the presence of significant traffic anomalies. Based on the Indonesian Cybersecurity Landscape 2023 published by BSSN, there were a total of 403,990,813 traffic anomalies, 4,001,905 Advanced Persistent Threat (APT) activities, and 1,011,209 ransomware activities (Indonesian Cybersecurity Landscape Annual Report 2023). This massive volume of attacks shows that the workload and the need for human resources capable of managing, detecting, and responding to threats are extremely high. At the same time, Indonesia has also experienced data breach incidents. Between 2004 and 2024, there were approximately 156.8 million leaked data records (Surfshark, Data Breach World Map). A BSSN report in 2003 recorded that 69% of data breaches occurred in the government administration sector. These problems have been strongly linked to vulnerabilities exploited through the human factor, including social engineering attacks such as phishing used to steal credentials.

In relation to this, the following section presents Indonesia's Cybersecurity Index data for 2024.

Table 1. National Cyber Security Index 2024

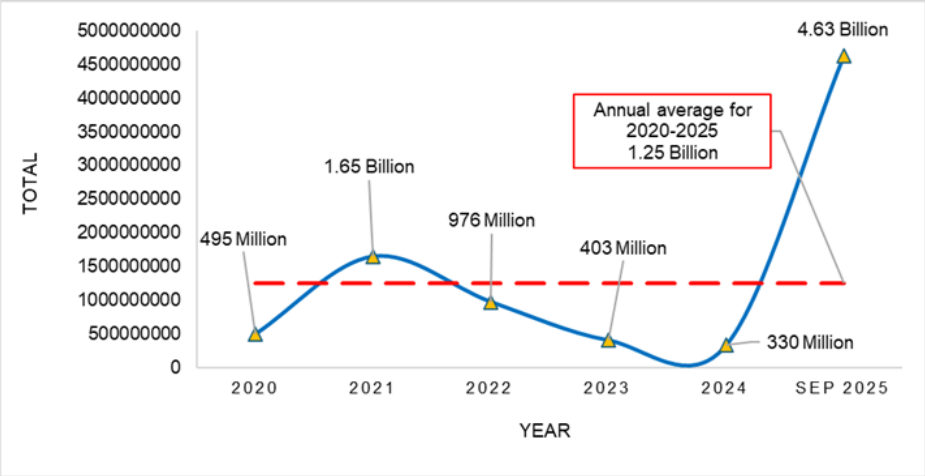
Peringkat ASEAN	Negara	Skor NCSI (dari 100)	Peringkat Global
1	Malaysia	79.22	22
2	Singapore	71.43	31
3	Thailand	64.94	45
4	Philippines	63.64	48
5	**Indonesia**	**63.64**	**49**
6	Brunei Darussalam	41.56	88
7	Vietnam	36.36	93
8	Cambodia	23.38	120
9	Laos	18.18	135
10	Myanmar	10.39	152

Source: e-Governance Academy (eGA), Estonia in NCSI (https://ncsi.ega.ee/ncsi-index/), 2024

Indonesia records the highest number of cyberattacks in Southeast Asia, driven by rapid economic growth and limited cybersecurity focus. Referring to the data, threats to Indonesia's cybersecurity exhibit clear anomalies in traffic throughout the 2020–2025 period. The number of anomalous traffic events fluctuated sharply—from 495 million in 2020, rising to 1.65 billion in 2021, then declining to 976 million in 2022 and 403 million in 2023, followed by a

slight drop to 330 million in 2024. However, by September 2025, the volume surged dramatically to 4.63 billion cases. Across 2020–2025, the three dominant types of traffic anomalies were malware-related activity, unauthorized access and system misconfiguration, and exploit activity. This overall pattern demonstrates a highly volatile threat landscape, indicating that the workload and the need for skilled human resources capable of managing, detecting, and responding to cybersecurity incidents are increasingly critical.

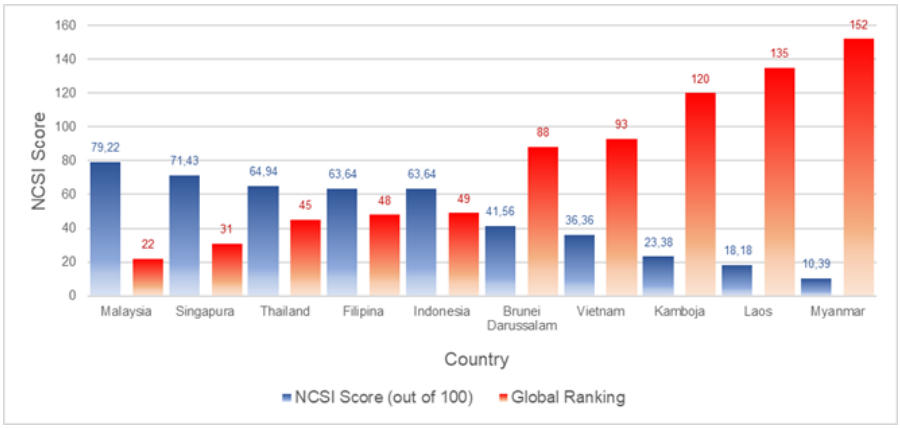
Figure 1. Traffic Anomaly Trend from 2020-2025



Source: BSSN, 2025

In June 2024, a ransomware attack on the National Data Center (PDN) disrupted critical public services such as immigration and airport operations, further revealing that the bulk of the data had no backup. More than 160 government agencies were affected by this attack and the attackers asked for $8 million in ransom to unlock the data, before eventually apologizing and returning the data back for free. BSSN's report notes that 69% of data breaches occurred in the government administration sector. These issues are strongly linked to vulnerabilities exploited through HR aspects, such as social engineering attacks like phishing to steal credentials. The amount and types of threats each year increases and varies, mostly dominated by malware and ransomware attacks, lack of data backup intensifies the issues and prolongs recovery, attacks are being made not only in the private sector but towards vital national functions and national banking institutions.

Figure 2. National Cyber Security Index Tahun 2024



Source: NCSI, 2024

The scores and rankings indicate a significant improvement, suggesting that there have been enhancements in national cybersecurity capacity. Although the trend of cyber threats in Indonesia shows a significant and massive increase, with attacks predominantly consisting of hacking attempts on web-based applications and phishing (BSSN, 2024).

Specific BSSN regulations emphasize mandatory human resource capacity-building policies for all government institutions and electronic system providers as the foundation for constructing national cyber defense (BSSN Regulation No. 9 of 2023). The national strategy for addressing cyber threats therefore focuses not only on technological aspects but also on strengthening the human resources pillar through the development of a competency framework and certified training programs (Sudarmadi & Runturambi, 2019).

In the theory of human factor in cybersecurity issues, humans are positioned as the weakest link in the information security system. No matter how advanced the technology and systems used are, security will fail if the human resources lack adequate awareness and caution. Modern cyber-attacks often target the human factor, which is easier to exploit than technical weaknesses. Therefore, it is necessary to have competitive advantage in human resources with high- level cyber expertise to utilize critical resources needed to build robust cyber resilience for national sovereignty. On the other hand, international cooperation also plays an important role in capacity building efforts. In defense diplomacy theory, cyber defense diplomacy serves two roles, to protect national interest in the digital realm, and to contribute to international security stability (Setyawan, 2019).

On the other hand, international cooperation also plays an important role in capacity-building efforts. Within the framework of defense diplomacy theory, cyber defense diplomacy can play a dual role: safeguarding national interests in the digital domain while at the same time contributing to the stability of international security (Setyawan, 2019). Indonesia has shown relatively active involvement in various international forums and cooperation related to cyber security, whether through bilateral, regional, or multilateral mechanisms. However, this involvement has not been fully supported by adequate domestic capacity, especially in terms of cyber security human resources (HR). A number of cyber incidents that have affected the country's strategic institutions show that the main problem does not always lie in the absence of regulations or policy frameworks, but rather in the limitations of cyber human resources who have the in-depth technical competence, operational readiness, and strategic understanding necessary to support defense and diplomacy in the cyber domain.

In national policy practice, strengthening cybersecurity is still often perceived as a matter of technology and administrative compliance. This approach, while important, tends to place cyber human resources solely as technical implementers, rather than as strategic assets of the state. In fact, within the framework of defense diplomacy, cyber security human resources are part of the instruments of national power that directly influence Indonesia's credibility, bargaining power, and position in international cooperation. Without human resources that have real and testable operational capabilities, cyber diplomacy risks remaining at a normative level, limited to attending forums and signing agreements without resulting in a substantial increase in defense capabilities.

Referring to Ministry of Defense Regulation No. 82 of 2014 on Cyber Defense, National Cyber Security is defined as efforts to maintain the confidentiality, integrity, and availability of information and all its supporting infrastructure at the national, cross-sectoral level. The problem of cyber vulnerabilities requires comprehensive handling involving multiple stakeholders. These efforts should not focus solely on technological infrastructure, but also on increasing HR capacity so that advanced threat intelligence can be conducted (Law No. 27 of 2022; BSSN, 2022). Thus, human resources are one of the most important elements in ensuring the implementation of cyber defense in accordance with established national policy directions. Specific BSSN regulations emphasize policies for HR capacity building that must be carried out by all government agencies and electronic system operators to build the foundation of cyber defense (BSSN Regulation No. 9 of 2023). The national strategy for dealing with cyber threats focuses not only on technological aspects, but also on strengthening the human resources pillar through the development of competency frameworks and certified training (Sudarmadi & Runturambi, 2019).

Although Indonesia has established BSSN and ratified the Personal Data Protection Law (PDP), the implementation of regulations and inter-agency coordination still faces serious challenges. Major cyber-attacks have demonstrated weak cyber security governance, limited data backups, and the non-optimal state of the national digital defense infrastructure (Reuters, 2024; Modern Diplomacy, 2024). Indonesia's defense diplomacy has so far only involved participation in multilateral forums such as ASEAN Regional Forum (ARF), or bilateral cooperation with partner countries, which tends to be more declarative than operationally strategic. Thus creating a gap between the need to strengthen national cyber security and the effectiveness of defense diplomacy in responding to real threats (Dig.Watch, 2025).

Previous studies have generally placed the issue of cybersecurity within the framework of national policy, regulatory strengthening, global index measurement, or patterns of international cooperation. This focus is evident, for example, in studies that highlight the strategies and challenges of implementing Indonesia's national cybersecurity policy (Islami, 2017; Sudarmadi & Runturambi, 2019), as well as research that analyzes the role of regional forums and multilateral cooperation in Indonesia's cyber diplomacy. particularly within the framework of ASEAN and the ASEAN Regional Forum (Setyawan & Sumari, 2019; Primawanti & Pangestu, 2020). Although these studies have made important contributions in mapping Indonesia's position in the global cyber landscape, discussions on cyber security human resource capacity as a key factor determining the effectiveness of defense diplomacy are still relatively limited. As a result, there is an analytical gap between the discourse on cyber diplomacy that is developing at the international level and the reality of domestic human resource readiness, which should be the main foundation of national cyber power.

Based on this gap, this study specifically focuses on strengthening the capacity of Indonesia's cybersecurity human resources in the context of defense diplomacy. This study is not intended to discuss cybersecurity in general, but rather to analyze how the competence, operational readiness, and strategic role of cybersecurity human resources affect Indonesia's ability to carry out defense diplomacy in the digital age. Thus, this study seeks to answer questions regarding the actual condition of Indonesia's cybersecurity human resource capacity, the extent to which these human resources function as instruments of state power in defense diplomacy, and the factors that hinder or support the optimization of this role.

This research examines the effectiveness of Indonesia's efforts to strengthen cybersecurity human resources during 2022–2024. The study seeks to answer three main questions: (1) What is the condition and capacity of Indonesia's defense human resources in facing cyber threats in the digital era? (2) How can a defense human resource development strategy be designed to strengthen diplomacy against cyber threats? (3) How can we build national cyber resilience through defense diplomacy?. Correspondingly, the objectives are to analyze existing HR challenges, formulate development strategies aligned with cyber diplomacy needs, and identify collaboration models involving the Ministry of Defense, Komdigi, BSSN, and international partners in strengthening national cyber capacity.

Through a qualitative analytical approach, this study is expected to contribute both conceptually and practically. Conceptually, this study affirms the position of cybersecurity human resources as a strategic element in defense diplomacy, not merely a complement to technical policies. Practically, the findings of this research are expected to serve as a reference in formulating strategies to strengthen cyber human resources that are more oriented towards operational readiness and increasing international credibility, so that Indonesia's defense diplomacy in the cyber realm does not stop at the normative level, but is able to produce real power for the interests of national defense.

2. Methods

The research data was obtained from two main sources, namely primary data and secondary data. Primary data was collected through in-depth interviews with informants selected purposively. Informants were individuals who had direct involvement or strategic understanding related to the development of cybersecurity human resources and the implementation of Indonesia's defense diplomacy. The group of informants included representatives of government institutions dealing with cybersecurity and defense, academics and cybersecurity experts, and practitioners involved in international cooperation in the field of cybersecurity.

2.1 Data Sources and Collection Techniques

The selection of informants was based on three main considerations. First, involvement in policy formulation or implementation of cybersecurity human resource strengthening programs. Second, experience in international cooperation or participation in cyber diplomacy forums. Third, understanding of both the technical and strategic dimensions of cybersecurity. With these criteria, this study sought to obtain perspectives that represent policy, operational, and strategic aspects in a balanced manner.

Secondary data was collected through documentation studies of various written sources, including national policy documents, official government reports, publications from institutions engaged in cybersecurity, and relevant academic literature. In addition, international cooperation documents, joint exercise implementation reports, and publications from regional and multilateral forums were analyzed to identify the extent to which such cooperation has produced concrete outputs that contribute to strengthening cybersecurity human resource capacity.

2.2 Data Analysis Techniques

Data analysis was conducted using thematic coding through the stages of data reduction, theme grouping, and analytical interpretation. Data obtained from interviews and documents were analyzed to identify patterns and main themes related to cybersecurity human resource capacity, particularly those concerning technical competence, operational readiness, and strategic roles in defense diplomacy.

In this study, cybersecurity human resource capacity is not narrowly understood as the possession of specific training or certification. Instead, capacity is analyzed based on qualitative indicators that reflect actual capabilities, including the ability to detect and respond to cyber incidents, the fulfillment of strategic roles and functions of cyber human resources in relevant institutions, involvement in joint exercises and international operational cooperation mechanisms, and the contribution of cyber human resources in the defense diplomacy process, both at the stage of formulating national positions and in the implementation of cooperation.

3. Results, Analysis, and Discussions

3.1 Results & Analysis

Human Resources Dimensions

The readiness of human resources to respond to cyber incidents quickly and in a structured manner is a critical indicator of cyber resilience, which must be supported by official incident management procedures (BSSN Regulation No. 1 of 2024). Research findings indicate that human resource development in Indonesia's Cybersecurity should be positioned not merely as a technical issue but as a crucial pillar of the national resilience strategy to achieve cyber resilience and national sovereignty. Indonesia's National Cybersecurity Strategy demonstrates a strategic vision of supporting Cyber Resilience, securing public services, enforcing cyber law, and securing the digital economy. Aligned with the RPJMN 2025–2029, the development of cybersecurity human resources is positioned not merely as a technical requirement but as a central pillar in strengthening national resilience, digital trust, and the protection of critical information infrastructure. Thus, the comprehensive strategy of BSSN and relevant ministries in HR development can involve various stakeholders. A critical asset for Indonesia is the formulation of a strong and internationally recognized strategic framework and the increased status of the GCI, which has already reached Tier-1, providing a positive impact in terms of commitment and sustainable capacity development that is massive, integrative, and solid.

The enhancement of Indonesia’s cybersecurity capacity can be achieved through a structured and strategic approach. Strategies and efforts for capacity building that can be undertaken within the framework of capacity strengthening include:

a) Developing the latest cybersecurity technologies, including advanced encryption, the implementation of AI and Machine Learning for threat detection and response, and the application of the Capacity Maturity Model (CMM) to measure national cybersecurity maturity.

b) Strengthening the security and resilience of critical infrastructure.
c) Intensifying international cooperation through diplomacy and public-private partnerships to share information and best practices as mandated by the Global Cybersecurity Index indicator.
d) Formulating a roadmap for HR capacity development supported by regulations and modern technology in accordance with BSSN's blueprint.

The readiness of a country or organization to face cyber threats can be measured by its maturity level. HR capacity development directly correlates with increased maturity scores, where a mature country is not only able to respond to incidents but is also proactive in prevention, policy development, and HR development.

BSSN

The National Cyber and Crypto Agency (BSSN) was established by the President in 2017 based on Presidential Regulation No. 53 of 2017 concerning the National Cyber and Crypto Agency, as amended by Presidential Regulation No. 133 of 2017. The formation of BSSN was an effort to reorganize the State Crypto Agency (Lemsaneg) into BSSN to ensure the implementation of government policies and programs in the field of cybersecurity. BSSN is tasked with carrying out cybersecurity effectively and efficiently, including developing and consolidating all elements related to cybersecurity.

BSSN is led by a Head and is positioned under, and responsible to, the President of the Republic of Indonesia. The establishment of BSSN considers the strategic nature of cybersecurity, which is a government sector that needs to be strengthened to support national economic growth and realize national security. The formation of BSSN is regulated as a centralization and coordination effort for cybersecurity functions, positioning this agency as the main actor responsible for developing human resource capacity across the ecosystem (Presidential Regulation No. 28 of 2021). Therefore, BSSN is an urgent necessity in the face of various issues and challenges related to cybersecurity and cryptography. The establishment of BSSN is expected to address current and future cybersecurity challenges in Indonesia.

In strengthening Indonesia’s cybersecurity posture, BSSN’s commitment is reflected in the operationalization of the Three Pillars of Cybersecurity—People, Process, and Technology—which serve as the foundation for building a professional, standards-based, and technologically empowered cybersecurity workforce. The People pillar is particularly central to BSSN’s HR development agenda, as it focuses on producing internationally certified cybersecurity professionals, including Red Team (offensive), Blue Team (defensive), and Yellow Team (DevSecOps) specialists. These certification and competency pathways are aligned with the broader national framework for enhancing skills in incident response, vulnerability management, digital forensics, and security operations.

This human-resource strengthening is further reinforced through the expansion of the National Cyber First Responder Team (TTIS), which functions as BSSN’s operational arm across ministries, regional governments, state-owned enterprises, academia, and critical national sectors. The hierarchical structure of TTIS—spanning national, sectoral, and organizational levels—enables BSSN to systematically deploy trained personnel who act as the first responder to cyber incidents before escalation occurs. The rapid growth of TTIS units, particularly within government administration sectors, demonstrates BSSN’s strategy to build a distributed and scalable cybersecurity workforce embedded directly in public institutions. These responders are trained not only in technical capabilities but also in adherence to standardized cybersecurity processes aligned with ISO 27001, GDPR, PCI-DSS, the PDP Law, and local regulatory requirements.

Together, the Three Pillars framework and the nationwide expansion of TTIS create a cohesive HR development ecosystem that integrates professional expertise, compliance-oriented processes, and advanced cybersecurity technologies. Through these initiatives, BSSN is institutionalizing a sustainable pipeline of skilled cybersecurity professionals capable of safeguarding Indonesia’s digital infrastructure, responding rapidly to security incidents, and supporting the nation’s long-term cyber resilience.

International Cooperation And Diplomacy

Indonesia's cybersecurity cooperation, both now and in the future, must be holistic, multi-sectoral, and proactive, shifting from a focus on passive defense to an adaptive national cyber resilience system. The cooperation framework can be implemented in both domestic and international sectors. First, Domestic Cross-Sector Cooperation, by implementing synergy within the country (whole-of-government and whole-of-society approach).

Table 1. Domestic Cross-Sector Cooperation Pillar

Cooperation Pillar	Current Focus	Future Focus (What needs to be improved)
Government-Government	The sustainability of ongoing cooperation (such as between BSSN and the Ministry of Defense, TNI, Polri, and BIN) for election security, cybercrime prevention, and cyber defense.	Integration and Centralized Command: BSSN must become a definitive and effective command center. Ensure that all ministries/agencies have a registered and operational CSIRT (Cyber Security Incident Response Team) and collaborate in sharing cyber threat information in real-time.
Public- Private	Cooperation in securing Critical Information Infrastructure (CII), such as the energy sector, finance (state-owned banks), and transportation, through MoUs and joint training.	Innovation and R&D Partnership: Encourage the establishment and development of the domestic cybersecurity industry through incentives. Collaboration between state-owned/private enterprises (such as banking, fintech) and BSSN for benchmarking high security standards.
Government-Academia/ Research	Programs such as the Digital Talent Scholarship (DTS) and cooperation for technical and non-technical training.	Curriculum & Advanced Research: Integrate cybersecurity curriculum and AI ethics nationally. Strengthen Research Centers to focus on AI-based cyber threats and new technologies..
Government-People	Public awareness campaigns and handling of cybercrime complaints (e.g., cybercrime).	Enhancing Critical Literacy: Focus on data literacy and advanced digital security to combat hoaxes, deepfakes, and AI-supported social engineering. Transform awareness into proactive action.

Source: Researcher Processed Data, 2025

Indonesia should leverage its active and independent foreign policy through the implementation of defense diplomacy to strengthen national cyber capabilities. Through constructive cooperation, this supports the enhancement of Indonesia's cybersecurity capacity.

Cybersecurity can no longer be viewed as the sole responsibility of a single institution, but rather as an ecosystem that requires cross-sector (multi-stakeholder) cooperation. This aligns with the fifth GCI pillar (Cooperation) and the ASEAN Digital Masterplan 2025, under which the effectiveness of Indonesia’s cyber defense depends on synergy between the government, the private sector, and academia. Such cooperation is crucial given the cross-border (borderless) and asymmetric nature of cyber threats.

Table 2. Cross- sectoral Cooperation International Level

Type of Cooperation	Main Objective	Relevant Partners
Bilateral	Capacity Building: Gaining knowledge transfer and the latest technology. Threat Information Sharing: Exchanging transnational cyber threat data.	United States, Australia, South Korea (KISA), Japan, and other developed countries with mature cybersecurity systems.
Regional (ASEAN)	Standardization and Joint Mitigation: Promote uniform cybersecurity standards and frameworks in the region. Strengthen ASEAN-CERT and cyber emergency response mechanisms.	All ASEAN member states, especially Singapore and Malaysia.
Multilateral	Normative Diplomacy: Actively participate in the formulation of international laws and norms in cyberspace (such as at the UN or regional forums) that are fair and prioritize national sovereignty.	UN Forum (GGE, OEWG), *Global Cybersecurity Index*(GCI/ITU).

Source: Researcher Processed Data, 2025

Cybersecurity can no longer be viewed as the sole responsibility of a single institution, but rather as an ecosystem that requires cross-sector (multi-stakeholder) cooperation. This aligns with the fifth GCI pillar (Cooperation) and the ASEAN Digital Masterplan 2025, under which the effectiveness of Indonesia’s cyber defense depends on synergy between the government, the private sector, and academia. Such cooperation is crucial given the cross-border (borderless) and asymmetric nature of cyber threats.

Regulatory And Policies Dimension

The formulation of the National Cybersecurity Strategy (SKSN) needs to be comprehensive, focusing not only on technical aspects but using a holistic approach that includes five main dimensions, often adopted from global models like the Global Cybersecurity Index (GCI) and reflected in Presidential Regulation (Perpres) No. 47 of 2023 on SKSN and Cyber Crisis Management. The framework can be centered on Human Resources, Planning, and Modern Technology by the National Cyber and Crypto Agency (BSSN) as the leading sector and coordinator. The formulation can begin with:

a) The urgency of drafting a comprehensive Cybersecurity Law (UU KS) (outside of the ITE Law) to fill the legal gap in terms of defense and countering cross-border and massive cyber threats.

b) Developing technical capabilities to detect, prevent, and respond to cyber incidents, including consistently implementing cybersecurity standards (such as SNI ISO/IEC 27032:2014) and integrating a national incident reporting system under BSSN.

c) Optimal coordination to avoid overlapping functions between BSSN, Ministries/Agencies, the Indonesian National Armed Forces (TNI), and the National Police (Polri). BSSN should act as the focal point coordinator in policy formulation and incident management.

d) Enhancing Human Resources (HR), increasing research, and raising awareness through massive education, training, and certification programs, as well as encouraging the domestic cybersecurity industry.

e) Strengthening government-private-academia cooperation and actively participating in global cybersecurity forums through the implementation of defense diplomacy

In policy terms, Indonesia already has a strong foundation through the Personal Data Protection Law (PDP Law) and the establishment of BSSN. This is reflected in the 2024 Global Cybersecurity Index (GCI) score, which places Indonesia in Tier 1 (Role-modelling). However, the national strategy must continue to bridge the gap between “legal commitment” (as captured by GCI) and “technical readiness” on the ground. Indonesia’s National Cyber Security Index (NCSI) score, which ranks fifth in ASEAN with 63.64 points, indicates that the National Cybersecurity Strategy (SKSN) should focus on strengthening critical information infrastructure and improving the reliability of incident response capabilities.

At the same time, Indonesia’s national strategy cannot stand alone; it must be aligned with the ASEAN Digital Masterplan (ADM) 2025 and the ASEAN Cybersecurity Cooperation Strategy 2021–2025. The fundamental pillars of ADM 2025 concerning Data Governance and Trusted Digital Services require Indonesia to enhance the capacity of its cybersecurity human resources as the backbone of the digital economy. The SKSN must incorporate dimensions of international cooperation and regional capacity building to address transnational threats such as ransomware and cyber espionage.

Ultimately, the success of the SKSN for the 2022–2024 period depends heavily on strengthening human resource capacity. This strategy must encompass **triple helix** collaboration (Government, Academia, and Industry) to close the digital talent gap. The primary focus should shift toward cyber resilience, namely the ability of systems to withstand, respond to, and rapidly recover from attacks, thereby reinforcing national cybersecurity.

Global Cybersecurity Index (GCI) Indonesia

The Global Cybersecurity Index (GCI) published by the International Telecommunication Union (ITU) functions as a global benchmark that provides a structured framework for the Government of Indonesia to identify weaknesses and formulate targeted human resource strategies in the cybersecurity domain. The role of the GCI in structuring Indonesia’s cybersecurity human resources can be analyzed through its assessment pillars, particularly the Capacity Development Measures pillar. The GCI assesses a country’s commitment to developing cybersecurity capabilities and capacities in a holistic manner. This pillar is directly related to human resources and consists of several key indicators. In 2017, Indonesia ranked 70th among 169 countries, with a score of 0.424, compared to the global average of 0.357.

The scope of the GCI is categorized into five pillars: legal, technical, organizational, capacity development, and cooperation.

In 2017, Indonesia was ranked 70th out of 169 countries, with a score of 0.424 compared to the global average score of 0.357. The GCI framework itself is organized into five pillars: legal, technical, organizational, capacity development, and cooperation, which together offer a comprehensive reference point for aligning national cybersecurity policies and human capital development initiatives.

Based on these considerations, the National Cyber and Crypto Agency (BSSN) and relevant ministries/agencies have adopted the five GCI pillars—including the Capacity Development pillar—as the main foundation for formulating the national cybersecurity strategy. This approach is reflected in the BSSN Strategic Plan for 2020–2024 and other national strategic plans.

The results of the GCI assessment assist Indonesia in identifying areas where human resources remain weak, whether in terms of quantity, quality, or awareness. If the score on the Capacity Development pillar is low, it provides a strong signal of the urgent need for investment in cybersecurity and defense education and training.

In the 2024 GCI, Indonesia has entered **Tier 1**, positioning it as a country with a strong cybersecurity commitment—comparable to advanced nations such as the United States, Japan, and Singapore. This result demonstrates growing cybersecurity commitment within the Asia-Pacific region, particularly among ASEAN countries. Key Tier 1 nations serve as role models. In terms of development, the cybersecurity policies of ASEAN member states are guided by two regional-level strategic documents, namely:

Table 2 Global Cybersecurity Index (GCI)

Key Indicators	**Relevance to Indonesia's Cybersecurity Human Resources**
Education and Training	Measures whether a country has adequate formal education programs (schools/universities) and professional training to produce cybersecurity experts.
Public Awareness Creation	Assesses the extent to which the government conducts campaigns or programs to raise security awareness among the public and internet users.
Research and Development (R&D)	Evaluates the presence of cybersecurity R&D activities supported by competent human resources, including within academic and government institutions.
Certification Bodies/Professional Standards	Reviews the existence of national institutions or schemes (such as SKKNI) for professional standardization and certification of cybersecurity human resources.

Source: International Telecommunication Union (ITU) diakses pada https://www.itu.int/pub/D-STR-GCI.01-2017 dan https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Based on these considerations, the National Cyber and Crypto Agency (BSSN) and relevant ministries/agencies have adopted the five GCI pillars—including the Capacity Development pillar—as the main foundation for formulating the national cybersecurity strategy. This approach is reflected in the BSSN Strategic Plan for 2020–2024 and other national strategic plans.

The results of the GCI assessment assist Indonesia in identifying areas where human resources remain weak, whether in terms of quantity, quality, or awareness. If the score on the Capacity Development pillar is low, it provides a strong signal of the urgent need for investment in cybersecurity and defense education and training.

In the 2024 GCI, Indonesia has entered **Tier 1**, positioning it as a country with a strong cybersecurity commitment—comparable to advanced nations such as the United States, Japan, and Singapore. This result demonstrates growing cybersecurity commitment within the Asia-Pacific region, particularly among ASEAN countries. Key Tier 1 nations serve as role models. In terms of development, the cybersecurity policies of ASEAN member states are guided by two regional-level strategic documents, namely:

ASEAN Cybersecurity Cooperation Strategy 2021–2025 — This strategy serves as the most relevant regional framework for the current period and focuses on five main dimensions:

Table 3 ASEAN Cybersecurity Cooperation Strategy Dimension

Dimensions	Regional Policy Focus
Advancing Cyber Readiness Cooperation	Strengthening cooperation among Computer Emergency Response Teams (CERTs) and conducting regional cyber exercises.
Strengthening Regional Cyber Policy Coordination	Coordinating cybersecurity and related digital policy issues, including the implementation of international cyber norms.
Enhancing Trust in Cyberspace	Promoting international cybersecurity standards (e.g., ISO) and encouraging digital inclusion as well as "cyber hygiene."
Regional Capacity Building	Developing modular, multidisciplinary, and multi-stakeholder approaches to cybersecurity capacity building.
International Cooperation	Engaging in multilateral collaboration with Dialogue Partners to achieve stability in cyberspace.

Source: ASEAN Cybersecurity Cooperation Strategy https://www.google.com/search?q=https://asean.org/book/asean-cybersecurity-cooperation-strategy-2021-2025/

1. **ASEAN Digital Masterplan (ADM) 2025** — This masterplan serves as the foundation for regional digitalization, with Cybersecurity and Data Governance as its fundamental pillars. Its goal is to achieve a leading Digital Community and Economic Bloc in ASEAN, supported by secure and transformative digital services, technologies, and ecosystems. (accessed from https://asean.org/book/asean-digital-masterplan-2025/)
2. **Overview of ASEAN Member States' Cybersecurity Policies** Although the details vary, the focus of key ASEAN countries' cybersecurity policies in 2024 is driven by similar regional challenges, including the rise of ransomware attacks, AI-driven scams, and national cybersecurity talent gaps.

Table 4 ASEAN Cybersecurity Policies

Countries	Status and Key Policies	Main Focus
Singapore	'Role-Modelling' Countries (Tier 1 GCI 2024). Their cybersecurity policies are considered the most mature.	Security of Critical Information Infrastructure (CII), Cyber Resilience, and Regional Leadership (through the CCA and capacity-building initiatives).
Indonesia	Jumping to Tier 1 in the 2024 GCI.	Personal Data Protection Law (PDP Law) (fully effective in 2024), formulation of the National Cybersecurity Strategy (under BSSN), and strengthening of the national cybersecurity human resources.
Malaysia	Tier 1 GCI 2024.	Finalization of the National Cybersecurity Policy (NCP), with a focus on private sector standards and cross-border data security.
Philippines	Implementing the National Cybersecurity Plan (NCSP) 2023–2028.	Strengthening cyber laws (for example, the impact of the SIM Card Registration Act), and efforts to balance privacy and security.
Vietnam	Tier 1 GCI 2024.	Strict Cybersecurity Law (2019), and a focus on local data control and national cyber sovereignty.

Source: ASEAN Cybersecurity Cooperation Strategy https://www.google.com/search?q=https://asean.org/book/asean-cybersecurity-cooperation-strategy-2021-2025/ .

ASEAN cybersecurity policies for 2024–2025 are shifting from merely establishing legal and technical foundations toward effective implementation and the harmonization of data governance, thereby driving large-scale human resource development to maintain Tier 1 status now and in the future.

3.2 Discussions

The findings of this study indicate that efforts to strengthen the capacity of cybersecurity human resources (HR) in Indonesia have shown notable progress in recent years, particularly through the role of the National Cyber and Crypto Agency (BSSN) as the national coordinating body. Nevertheless, this capacity development has not yet fully kept pace with the increasing complexity and escalation of cyber threats faced by the state. Based on interviews with practitioners and policy analysts, a gap remains between formal capacity-building initiatives and the actual operational readiness of cybersecurity personnel in supporting Indonesia's defense and defense diplomacy objectives.

ASEAN cybersecurity policies for 2024–2025 are shifting from merely establishing legal and technical foundations toward effective implementation and the harmonization of data governance, thereby driving large-scale human resource development to maintain Tier 1 status now and in the future.

Within the context of cyber defense, human resource capacity cannot be reduced merely to the number of training, certifications, or the existence of regulatory frameworks. Instead, capacity should be reflected in testable operational capabilities, such as the speed and accuracy of incident detection and response, the effectiveness of inter-agency coordination, and the ability to secure critical information infrastructure. The ransomware attack on the National Data Center (PDN) in 2024 serves as a concrete illustration that limitations in human resources both in terms of technical competence and procedural readiness remain a critical vulnerability in Indonesia's national cyber resilience. Several informants noted that the handling of this incident also affected the level of trust and perception of Indonesia's cyber capacity among international partners.

These findings are consistent with a number of studies and policy documents that emphasize cybersecurity human resource development as a key pillar of national cyber resilience. A study by *European Union Agency For Cybersecurity* for example, shows that countries with high levels of cybersecurity workforce readiness tend not to rely solely on formal training, but also emphasize incident-based simulations, tiered certification schemes, and cross-institutional professional networks (European Union Agency For Cyberseucirty, 2023). In the Indonesian context, this approach aligns with BSSN's (2022) emphasis on an ecosystem-based model for cybersecurity human resource development, integrating government, academia, and the private sector. However, this study finds that such integration remains partial, resulting in suboptimal knowledge transfer and limited improvements in operational capacity.

Analysis of ASEAN cybersecurity cooperation documents, reinforced by interviews with cybersecurity researchers, further reveals that Indonesia continues to face challenges in developing personnel with advanced cybersecurity skills, such as cyber threat intelligence, digital forensics, and incident command leadership. This finding supports Klimburg's (2017) argument that a state's cyber capacity is not determined primarily by technology or regulation, but by the quality of human resources capable of operationalizing policy and technology during crises (Klimburg, 2011). Expanding the number of personnel without strengthening strategic competencies risks creating a false sense of readiness in national cyber defense.

From a defense diplomacy perspective, these findings underscore that cyber diplomacy cannot be separated from domestic human resource readiness. Defense diplomacy in the cyber domain should not be understood merely as participation in international forums or the signing of memoranda of understanding, but rather as the ability of a state to demonstrate tangible capacity as a credible and reliable partner (Johann Ole Willers, 2026). Without cybersecurity personnel possessing strong operational capabilities, international cooperation risks remaining normative and symbolic, failing to produce concrete outcomes such as sustained knowledge transfer, effective joint exercises, or integrated incident response mechanisms.

As the national coordinator for cybersecurity, BSSN has established an important institutional foundation through the development of the Three Pillars of Cybersecurity framework (People, Process, and Technology) and the formation of the National Cyber First Responder Team (TTIS). These initiatives reflect a relevant policy direction toward building a more structured cybersecurity human resource ecosystem. Nonetheless, the study finds that implementation continues to face significant challenges, particularly with regard to the uneven distribution of competencies across institutions, insufficient cross-sectoral coordination, and the lack of continuity in developing advanced skills required to respond to strategic cyber threats.

When compared with international literature, the findings of this study confirm patterns identified by Nye & Libicki, who argue that cyber power constitutes an integral component of national power and is heavily dependent on the quality of human capital (Libicki, 2014). States with relatively mature cybersecurity human resource capacity, such as the United States and several European Union countries, are able to leverage cyber diplomacy not only as a normative instrument but also as a strategic tool to shape rules, build coalitions, and strengthen deterrence. In contrast, states with limited human resource capacity tend to occupy reactive and norm-following positions in global cyber governance.

The implications of these findings for Indonesia's defense diplomacy are substantial. Strengthening cybersecurity human resource capacity not only enhances domestic resilience, but also determines Indonesia's credibility as a strategic partner in international cyber defense cooperation. Cybersecurity personnel with strong operational and

strategic capabilities enable Indonesia to play a more active role in norm-setting processes, joint exercises, and the development of cross-border incident response mechanisms. Accordingly, investment in cybersecurity human resource development should be positioned as an integral component of Indonesia's defense diplomacy strategy, ensuring that national interests can be effectively articulated and advanced within an increasingly complex global cybersecurity environment.

4. Conclusion and Recommendations

4.1 Conclusion

The research findings on Enhancing the Capacity of Human Resources (HR) in Cybersecurity to Address Cyber Threats in Indonesia for the period 2022–2024 indicate that:

1. Capacity has indeed increased; however, this improvement has not kept pace with the rate of growth and complexity of cyber threats, which have risen significantly compared to existing technology and human resources. As a result, the capacity of competent cybersecurity personnel remains a critical issue.
2. The implementation of cross-institutional collaboration plays a strategic role, as cybersecurity requires a holistic and integrated approach. This includes building awareness or a culture among the public so that they understand and become part of Indonesia's cyber defense and security efforts.
3. Commitment to and continuity of international cooperation through defense diplomacy are key to remaining competitive in capacity building. Therefore, such cooperation must be continuously strengthened and expanded at the bilateral, regional, and multilateral levels.

4.2 Recommendations

Based on the above conclusions, the following strategic recommendations are proposed to strengthen national cyber resilience through human resource development. The government needs to allocate budget for advanced, globally recognized cybersecurity certifications and for the modernization of national cyber technologies or tools for cybersecurity personnel at BSSN. Commitment to and continuity of cooperation with various strategic stakeholders must be enhanced. In addition, these efforts can be supported through the strengthening of regulations being prepared, such as the Draft Cybersecurity Law, which can provide a comprehensive legal umbrella to protect national cyberspace—particularly Critical Information Infrastructure—from various forms of cyber threats, as well as establish clear compliance obligations for all relevant parties.

References

A. T. Kearney. (2018). *Cybersecurity in ASEAN: An urgent call to action*. A. T. Kearney.

Arianto, A. R., & Anggraini, G. (2019). Membangun pertahanan dan keamanan siber nasional Indonesia guna menghadapi ancaman siber global melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan dan Bela Negara*, 9(1), 1–17.

Asosiasi Penyelenggara Jasa Internet Indonesia. (2024, February 7). *Jumlah pengguna internet Indonesia tembus 221 juta orang*. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Badan Keahlian DPR RI. (2022). *Penguatan keamanan siber nasional melalui peningkatan sumber daya manusia (SDM) bidang siber*. Budget Issue Brief Politik dan Keamanan DPR RI, 2(7). https://berkas.dpr.go.id/pa3kn/analisis-tematik-apbn/public-file/bib-public-112.pdf

Badan Siber dan Sandi Negara. (2022). *Lanskap keamanan siber Indonesia tahun 2022*. BSSN.

Badan Siber dan Sandi Negara. (2024). *Lanskap keamanan siber Indonesia tahun 2024*. BSSN.

Badan Siber dan Sandi Negara. (2025). *Laporan hasil monitoring National Operation Security Center*. BSSN.

Chakravarti, J., & Ross, R. (2023, August 2). Indonesia hardest hit by cyberattacks in the region. *Bank Information Security*. https://www.bankinfosecurity.asia/indonesia-hardest-hit-by-cyberattacks-in-region-a-22720

Djari, M. L. (2021). *Offline to online: 75 tahun Badan Siber dan Sandi mengabdi*. BSSN.

E-Governance Academy. (2024). *National Cyber Security Index (NCSI): Indonesia*. https://ncsi.ega.ee/ncsi-index/

European Union Agency For Cyberseucirty. (2023). *Enisa Threat Landscape 2023.* Enisa. From https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Febriansyah, M. F., Adriyanto, A., & Miftach, F. (2020). Strategi Badan Siber dan Sandi Nasional dalam menghadapi ancaman siber terhadap Sistem Pemerintahan Berbasis Elektronik. *Jurnal Peperangan Asimetris*, 6(2).

International Telecommunication Union. (2021). *Global cybersecurity index 2020*. ITU.

Islami, M. J. (2017). Tantangan dalam implementasi strategi keamanan siber nasional Indonesia ditinjau dari penilaian Global Cybersecurity Index. *Jurnal Masyarakat Telematika dan Informasi*, 8(2), 137–144.

Johann Ole Willers, L. G. (2026). Diplomacy in the Age of Expertise: the cASE OF cYBER dIPLOMACY. *International Affairs*. doi:https://doi.org/10.1093/ia/iiaf271

Klimburg, A. (2011). The Whole of Nation in Cyberpower. *Georgetown Journal of International Law*. From https://www.jstor.org/stable/43133826

Libicki, M. C. (2014). Why Cyber War Will Not and Should Not Have Its Grand Strategist. *Strategic Studies Quarterly*. From https://www.jstor.org/stable/26270603

Komisi I DPR RI. (2024). *Laporan singkat rapat kerja dengan Menteri Komunikasi dan Informatika dan Kepala BSSN terkait penanganan gangguan Pusat Data Nasional (27 Juni 2024)*.

Kristianti, L., & Adji, R. A. (2023, January 19). BSSN records decrease in cyberattacks in 2022. *Antara News*. https://en.antaranews.com/news/270015/bssn-records-decrease-in-cyberattacks-in-2022

Lembaga Kajian dan Konsultasi Fakultas Hukum Universitas Indonesia. (2023, June 16). *Bank BSI pasca serangan siber: Mengungkap potensi kompensasi bagi nasabah*. https://lk2fhui.law.ui.ac.id/portfolio/bank-bsi-pasca-serangan-siber-mengungkap-potensi-kompensasi-bagi-nasabah/

National Institute of Standards and Technology. (2020). *NICE cybersecurity workforce framework (NIST SP 800-181)*. NIST.

Primawanti, H., & Pangestu, S. (2020). Diplomasi siber Indonesia dalam meningkatkan keamanan siber melalui ASEAN Regional Forum. *Global Mind*, 2(2). https://doi.org/10.53675/jgm.v2i2.89

Presiden Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* (sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024).

Presiden Republik Indonesia. (2018). *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*.

Presiden Republik Indonesia. (2021). *Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara*.

Presiden Republik Indonesia. (2022). *Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital*.

Presiden Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

Reuters. (2024, July 12). Indonesia says it has begun recovering data after major ransomware attack. *Reuters*. https://www.reuters.com/technology/cybersecurity/indonesia-says-it-has-begun-recovering-data-after-major-ransomware-attack-2024-07-12/

Runturambi, A. J. S., & Sutiadi, D. (2013). *Manajemen sekuriti: Karakteristik lokasi dan desain*. Universitas Indonesia.

Setyawan, D. P., & Sumari, A. D. W. (2019). *Diplomasi pertahanan Indonesia dalam pencapaian keamanan siber melalui ADMM-Plus tahun 2014–2019* (Tesis). Universitas Pertahanan Indonesia.

Smart City Gunungkidul Kabupaten. (2024, September 14). *Peningkatan Indeks Masyarakat Digital Indonesia 2024*. https://smartcity.gunungkidulkab.go.id/2024/09/14/peningkatan-indeks-masyarakat-digital-indonesia-2024

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) dalam menghadapi ancaman siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, 2(2), 157–178.

Kementerian PPN/Bappenas. (2022). Strategi Pembangunan Sumber Daya Manusia Unggul dalam Kerangka Transformasi Digital Nasional. *Jurnal Perencanaan Pembangunan: The Indonesian Journal of Planning and Development*, 6(2), 145-162.

Kementerian PPN/Bappenas. (2023). *Evaluasi Paruh Waktu Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020-2024: Fokus Ketahanan Siber dan Digitalisasi*. Jakarta: Bappenas.