Journal of World Science
Vol. 5, No. 11, November 2026, pp 957-969
E-ISSN: 2828-9307
https://doi.org/10.58344/jws.v5i11.1721

Optimizing the Readiness of Indonesian Air Force Personnel in Facing the Rapid Development of Information Technology in the Era of Cyber Warfare

Indra Paulus*, Usni Hasanudin
Universitas Muhammadiyah Jakarta, Indonesia
Email : Indrapaulus08@gmail.com*, Usnihasanudin@gmail.com

Keywords:
cyber warfare;
capacity;
competence;
recruitment.

This is an open access article under the CC BY-SA license.

Copyright © 2026 by Author. Published by Riviera Publishing

ABSTRACT

The rapid advancement of information technology has established cyberspace as a strategic domain of national defense. Cyber warfare threats affect not only technical systems but also the continuity of military operations and the security of critical information infrastructure. As a key component of national air defense, the Indonesian Air Force must maintain adequate cyber resilience to address increasingly complex, adaptive, and strategically significant cyber threats. Personnel competencies and recruitment strategies are therefore critical factors in strengthening cybersecurity readiness. This study aimed to assess the cyber resilience readiness of the Indonesian Air Force, focusing on the capacity and competencies of cybersecurity personnel and existing recruitment practices in response to technological advancements and evolving cyber warfare threats. The study employed a qualitative case study approach, incorporating in-depth interviews, policy document analysis, and an examination of cyber incident records within the Indonesian Air Force. The findings indicated that cybersecurity education and training programs conducted by the Indonesian Air Force had established a foundation of essential competencies in information security and cyber incident response. However, personnel capabilities in advanced cybersecurity disciplines, including cyber threat intelligence, digital forensics, and malware analysis, remained limited. The study concluded that strengthening the cyber resilience readiness of the Indonesian Air Force required an integrated approach involving enhanced personnel capacity, specialized competency development, and the modernization of recruitment strategies aligned with information technology and cybersecurity specializations.

INTRODUCTION

The rapid advancement of information technology has significantly influenced various aspects of society, including national defense and security (Flor-Unda et al., 2025). Digital transformation, driven by technologies such as big data analytics, artificial intelligence (AI), cloud computing, and the Internet of Things (IoT), has reshaped socioeconomic structures and modern military strategies (Schwab, 2017). In the era of cyber warfare, technological capabilities are no longer merely supporting components of military operations but have become strategic assets that influence operational effectiveness and superiority in the cyber

domain. This transformation aligns with Castells' (2010) theory of the network society, which emphasizes the role of information and communication technologies in shaping social structures and power relations. It also reflects the perspective of United Nations Secretary-General António Guterres, who described digital technology as a transformative force in global development, with implications for national security and defense (Guterres, 2018). While these technological advancements create opportunities for innovation and improved defense capabilities, they also introduce complex security challenges that require continuous improvements in personnel readiness, technical expertise, and organizational adaptability, particularly within the air defense sector.

The Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU), as a principal component of Indonesia's national defense in the air domain, plays a strategic role in protecting national airspace and maintaining operational readiness amid increasingly complex security threats. Consequently, its defense capabilities must extend beyond conventional military assets to incorporate advanced digital technologies throughout air operations. In particular, Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems are essential for supporting timely, accurate, and coordinated military decision-making. The integration of these systems requires reliable cybersecurity infrastructure and personnel capable of maintaining information security, operational continuity, and resilience against evolving cyber threats. This strategic requirement is consistent with Law No. 3 of 2002 concerning State Defense, particularly Article 20(2), which addresses the mobilization and utilization of national resources in support of defense capabilities (Law of the Republic of Indonesia Number 3 of 2002, 2002).

Alongside the increasing digitalization of military operations, cyber threats targeting the Indonesian Air Force's vital information infrastructure (Infrastruktur Informasi Vital, IIV) have become more diverse and operationally significant. Cyber incident monitoring records indicated that most incidents reported between 2022 and 2025 were successfully addressed by the Indonesian Air Force Cyber Unit (Satuan Siber Angkatan Udara, Satsiberau). However, several incidents required multiple days to resolve, potentially compromising the confidentiality, integrity, and availability (CIA) of information systems and disrupting the continuity of organizational operations. As presented in Table 1, a total of 35 cybersecurity incidents were recorded during the observation period, including sensitive data exposure, website defacement, cross-site scripting (XSS), SQL injection, and ransomware attacks. The recorded incidence increased substantially in 2024, highlighting the growing importance of strengthening cybersecurity preparedness, incident response capabilities, and specialized personnel competencies within the Indonesian Air Force (Firdini et al., 2024; Sutomo et al., 2025).

Table 1. Cyber Attack Incidents of the Indonesian Air Force, 2022–2025

No	Year	Types of Cyberattacks	Number of Incidents
1	2022	Sensitive Data Exposure	1
2	2023	Sensitive Data Exposure, Web Defacement, Cross Site Scripting	8
3	2024	Web Defacement, Sensitive Data Exposure, SQL Injection	18
4	2025	Web Defacement, Sensitive Data Exposure, Ransomware	8

Source: Satsiberau

These conditions indicate that cyber threats targeting Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) information systems are becoming increasingly complex and adaptive. To safeguard its vital information infrastructure (Infrastruktur Informasi Vital, IIV), the TNI AU has implemented an information security management system aligned with the Indonesian National Standards (Standar Nasional Indonesia, SNI) (Damanik et al., 2023; Triharto et al., 2024). However, the effectiveness of this system depends not only on technological infrastructure but also on personnel competencies, cybersecurity awareness, and adherence to established information security procedures. The ability of cybersecurity personnel to effectively operate, manage, and protect information systems remains a significant challenge in strengthening the professionalism of the Indonesian National Armed Forces (Tentara Nasional Indonesia, TNI) (Laksono et al., 2026; Sarjito, 2024). In this context, military professionalism encompasses not only discipline and operational competence but also awareness of emerging cyber threats, proficiency in cybersecurity risk assessment, and consistent implementation of information security protocols.

In practice, human resource limitations remain a major obstacle to strengthening cybersecurity readiness within the TNI AU. Cybersecurity knowledge and technical competencies vary among personnel of the Indonesian Air Force Cyber Unit (Satuan Siber Angkatan Udara, Satsiberau), while the availability of personnel with specialized cybersecurity qualifications and opportunities for continuous professional development remains limited. These challenges arise from two interconnected issues. First, personnel capabilities in managing and securing defense information systems remain insufficient, partly because existing military education and training curricula do not adequately emphasize advanced cybersecurity competencies (Hardiyanto & Yosepha, 2025; Prümmer et al., 2024). Second, existing recruitment practices remain primarily oriented toward general military selection criteria, with limited consideration of applicants' educational backgrounds and specialized qualifications in information technology and cybersecurity (U.S. Department of Defense, 2023; U.S. Government Accountability Office, 2022). Furthermore, collaboration with universities, technical training institutions, and professional cybersecurity communities as potential sources of qualified personnel remains underdeveloped. Consequently, expertise in critical technological fields, including artificial intelligence, big data analytics, digital forensics, and cyber threat intelligence, remains limited. These deficiencies may hinder personnel development, succession planning, and the institutional strengthening of cybersecurity units as threats involving artificial intelligence, big data technologies, and Internet of Things (IoT) systems continue to evolve.

These circumstances reveal a substantial gap between existing conditions (das Sein) and the desired normative standards (das Sollen) of cybersecurity readiness within the TNI AU. Under current conditions, personnel readiness to address rapid technological advancements and increasingly sophisticated cyber warfare threats remains constrained by limitations in technical expertise, specialized training, and recruitment mechanisms. Ideally, TNI AU personnel should possess advanced digital literacy, specialized cybersecurity competencies, and the operational capabilities necessary to conduct air defense and cyberspace operations effectively, adaptively, and through a defense-in-depth approach. Failure to address these institutional and human resource challenges could undermine the protection of vital information infrastructure,

compromise operational continuity, and impede efforts to strengthen military professionalism in the digital era.

Against this background, this study aimed to (1) assess the capacity and competencies of TNI AU cybersecurity personnel in responding to rapid information technology developments and evolving cyber warfare threats and (2) examine existing TNI AU recruitment practices and their alignment with the growing demand for specialized expertise in information technology and cybersecurity. The findings were expected to provide strategic recommendations for improving cybersecurity personnel development, strengthening specialized recruitment and training mechanisms, and enhancing institutional cyber resilience. Ultimately, the study sought to contribute to the professionalization of TNI AU personnel, the effectiveness of military cyber defense capabilities, and the strengthening of Indonesia's national cybersecurity resilience.

METHOD

The study was conducted at the Indonesian Air Force Cyber Unit (Satuan Siber Angkatan Udara, Satsiberau), Headquarters of the Indonesian Air Force, Cilangkap, East Jakarta. The research was carried out over five months, covering proposal preparation, data collection, analysis, and thesis writing, as outlined in Table 2.

This study employed a qualitative analytical approach with a case study design, focusing on the readiness of Indonesian Air Force personnel to address developments in information technology and emerging cyber warfare threats. The investigation examined personnel-related factors, including competencies, professionalism, and recruitment practices, as well as technological and organizational factors, particularly technology adoption, institutional policies, operational procedures, and information security systems. Data were collected through in-depth interviews, field observations, and an examination of internal Indonesian Air Force documents concerning cybersecurity training, recruitment policies, and information technology utilization. The collected data were analyzed thematically to identify recurring patterns, institutional constraints, and opportunities for strengthening cybersecurity personnel readiness (Sugiyono, 2014). The case study approach enabled an in-depth examination of personnel competencies, interactions, organizational dynamics, and the utilization of information technology within the Indonesian Air Force. Multiple sources of evidence, including interviews, internal policy documents, training reports, and information security records, were used to support the analysis and strengthen the credibility of the findings.

Table 2. Research Implementation Schedule

Yes	Activities	Month 1	Month 2	Month 3	Month 4	Month 5
1	Guidance	✓	✓	✓	✓	✓
2	Data Collection		✓	✓		
3	Proposal Writing	✓	✓			
4	Research & Data Analysis			✓	✓	
5	Thesis / Manuscript Preparation				✓	✓

Yes	Activities	Month 1	Month 2	Month 3	Month 4	Month 5
6	Thesis Exam & Improvement					✓

Source: Managed by Researcher (2025)

Informants were selected using a purposive sampling technique based on their knowledge, expertise, and experience in cybersecurity personnel management, recruitment, competency development, and the utilization of advanced information technology within the Indonesian Air Force. Three key informants participated in the study: the Deputy Intelligence Assistant to the Chief of Staff of the Air Force (Waasintel Kasau), First Marshal TNI Ir. Yudy Mandega R., M.Tr.(Han)., IPM; the Head of Section VI for Signals Intelligence and Cybersecurity (Paban VI Sandi dan Siber Sintelau), Colonel Sus Makmur Siahaan, M.Kn., M.Han.; and the Deputy Commander of the Indonesian Air Force Cyber Unit (Wadan Satsiberau), Colonel Sus Theodorus. Data were collected through three primary techniques (Satori & Komariah, 2020; Sugiyono, 2014). First, semi-structured, in-depth interviews were conducted to obtain detailed information regarding personnel readiness, cybersecurity competencies, recruitment practices, and institutional challenges within Satsiberau. Second, field observations were conducted to examine the relationship between the educational and training processes at Skadik 506 and operational practices within Satsiberau. Third, documentation was used to collect supporting information from Indonesian Air Force cybersecurity policies, educational curricula, training reports, and cyber incident records.

Data analysis followed the interactive model of Miles and Huberman, as cited in Sugiyono (2014), comprising four stages: data collection, data reduction, data presentation, and conclusion drawing and verification. Data validity was established through source triangulation by comparing information obtained from different informants and verifying interview findings against relevant official documents and institutional records. This process helped identify consistencies, discrepancies, and complementary information across the data sources, thereby strengthening the credibility of the research findings.

Table 3. Data Analysis Engineering Component Matrix (Qualitative Interactive)

Stages of Analysis	Operational Description of Activities
Data Collection	The process of collecting primary and secondary data through in-depth interviews, participatory observation, and organizational documentation studies.
Data Reduction	Select, simplify, abstract, and transform raw data from Field notes and interview transcripts.
Data Presentation	Coordinate a set of information in the form of narrative texts, comparative tables, and a thematic matrix to facilitate the drawing of conclusions.
Conclusion Drawn/Verification	Establish the meaning of the analyzed data, test the correctness and suitability of the data through verification during the research.

Source: Synthesis of Data Analysis (Sugiyono, 2014)

RESULTS AND DISCUSSION

Overview of Research Objects

In this study, the object studied is the readiness of TNI AU cyber personnel in facing the development of information technology in the era of cyber warfare, especially in

supporting the security of Vital Information Infrastructure (IIV) within the TNI AU. The focus of the research is directed at personnel who serve in the cyber field, both in operational units, intelligence units, and education units, who have a strategic role in maintaining the security of information systems, data, and TNI AU networks. The selection of cyber personnel as the object of research is based on their role as the main actor in the implementation of cyber defense policies, the operation of information security systems, and the handling of cyber incidents. In the context of increasingly complex and adaptive cyber warfare threats, personnel readiness is not only determined by mastery of technology, but also by professional competence, operational preparedness, and the ability to adapt to the dynamics of digital threats. Therefore, this study places cyber human resources as a key factor in supporting information technology-based air defense resilience.

Cyber personnel owned by the Indonesian Air Force are spread across various work units, with the main role being in units that have the functions of information security, network management, and handling cyber incidents. Cyber personnel in the implementation of their duties are directly involved in system monitoring, vulnerability detection, response to cyber attacks, and system recovery after cyber attack incidents. In the face of the rapid development of information technology, Indonesian Air Force cyber personnel are faced with challenges in the form of increasing complexity of cyber threats, such as web defacement, data leaks (sensitive data exposure), malware attacks, and ransomware. These threats have the potential to disrupt the confidentiality, integrity, and availability of information, as well as affect the continuity of organizational functions. Therefore, the readiness of cyber personnel is not only understood as technical capabilities, but also includes mental preparedness, understanding of information security policies, and the ability to work in cross-unit coordination.

Capacity and Competence of Cyber Personnel

Based on the results of interviews with informants, it was found that the TNI AU's cyber education and training policies have been directed as an integral part of strengthening the country's defense preparedness. Waasintel Kasau, Yudi (2025), stated that the capacity of TNI Air Force cyber personnel in general is already at an adequate operational level for handling basic incidents, but competence in the aspects of advanced threat analysis and cyber intelligence is not evenly distributed. This is emphasized by Paban VI Sandi and Siber Sintelau, Makmur (2025), who stated that the mastery of advanced cyber techniques such as malware analysis, dark web monitoring, and cyber threat intelligence is still limited to a small number of personnel.

Table 4. Participation of Indonesian Air Force Personnel in Cyber Education

Yes	Education Name	Number of Personnel
1	Cyber Suspect & Intelligence Satinduk Bais TNI	13
2	Suspa Cyber Defense Kodiklat TNI	2
3	Southeast Asia Alumni Cyber Security Training Program	1

Yes	Education Name	Number of Personnel
4	Susba Cyber & Intelligence Satinduk Bais TNI	26
5	Susba Siber Skadik 501 Wingdik 500/General	10

Source: Sub-Directorate of Science and Technology

Wadansatsiberau, Theodorus (2025), explained that technically personnel are able to carry out network security, but the conceptual understanding of cyber warfare as an integrated operation still needs to be strengthened. He also presented cyber certification data owned by personnel.

Table 5. List of Cyber Certification Ownership of TNI Air Force Personnel

Yes	Cyber Certification Name	Number of Personnel
1	Certified Ethical Hacker (CEH)	8
2	Certified Network Defender (CND)	3
3	Certified Penetration Testing Professional (CPENT)	2
4	Junior Penetration Test (JPT)	12
5	Certified Hacking Forensic Investigator (CHFI)	1
6	L1 SOC Analyst	2
7	Assistant Information Security Auditor (AAKI)	3

Source: Satsiberau

Cyber education data in Skadik 506/Wingdik 500 in 2025 provides a comprehensive picture of the distribution of officers, non-commissioned officers, and enlisted men who participate in IT and cyber vocational training.

Table 6. List of Education in Skadik 506/Wingdik 500 (Year 2025)

Yes	Education Name	Fort	Go	Plot	PNS	Dik Time
1	1st Cybersecurity Basics Course	6	22	21	-	3 months
2	33rd Computer Operator Course	-	7	10	-	2 months
3	Vocational Management Officer Course (IT) Ke-27	-	13	-	-	3 months
4	14th Tamtama Lek (IT) Basic Vocational School	-	-	24	-	5 months
5	8th Tamtama Lek (IT) Advanced Vocational Course	-	-	13	-	3 months
6	44th Bintara Lek (IT) Vocational School	-	36	-	-	5 months
7	23rd Computer Programmer Course	10	-	-	-	2 months
8	8th Computer Network Administrator Course	10	-	-	-	2 months

Yes	Education Name	Fort	Go	Plot	PNS	Dik Time
9	18th Computer Technician Course	-	11	10	-	2 months
10	Cybersecurity Management Officer A-1 Course	20	-	-	-	1 month
11	1st Junior Penetration Tester Course	3	4	2	-	2 months
12	1st LV1 Security Operation Center Analyst Course	2	5	4	-	1 month
13	1st Digital Forensic Course	1	4	5	-	1.5 months
14	45th Bintara Lek (IT) Vocational School	-	55	-	-	3 months
15	Cyber Operations Commander TNI Air Force A-1	24	6	-	-	1 month

Source: Skadik 506/Wingdik 500

Cyber Personnel Recruitment Patterns

The current recruitment pattern of TNI AU cyber personnel still follows the general soldier recruitment system, with an emphasis on uniform physical requirements, age, and personal condition. Waasintel Kasau Yudi (2025) and Paban VI Sandi and Siber Sintelau Makmur (2025) emphasized that the recruitment mechanism has not been fully adjusted to attract civilian professional cyber practitioners. For comparison, military cyber institutions at the TNI Headquarters level (Satsiber TNI) have begun to initiate special recruitment of career officers in the cyber field.

Table 7. Public Information on Special Recruitment in the Cyber Sector by the TNI Task Force (Conversion Figure 1)

Information Element	Publication Description / Recruitment Policy
Program Title	Acceptance of Prospective Career Soldier Officers (PA PK) TNI Special Cyber FY 2025
Organizer	Indonesian National Army Cyber Unit (Satsiber TNI)
News Sources	Medcom.id (Publication 04 September 2025)
Policy Objectives	Attracting cyber specialist talents directly from professionals/university graduates to meet the operational needs of cyber defense.

Source: Medcom. en (Managed by Researchers, 2025)

The development of cyber commands and forces in various global countries also shows specific organizational specialization and recruitment tendencies.

Table 8. Cyber Force/Command Structure in Various Global Countries (Conversion Figure 2)

Country	War/Cyber Defense Entity Name	Organizational Patronage
Singapore	Digital and Intelligence Service (DIS)	Singapore Armed Forces
United States	United States Cyber Command (USCYBERCOM)	U.S. Department of Defense
English	The National Cyber Force (NCF)	UK Ministry of Defence

Country	War/Cyber Defense Entity Name	Organizational Patronage
France	Cyber Defence Command	Ministry of the Armed Forces France
China	PLA Strategic Support Force	Chinese Army/Armed Forces

Source: Antara, PinterPolitik (Managed by Researcher, 2025)

Cyber Personnel Capacity and Competency Analysis

Policies on increasing the capacity and competence of cyber personnel are an integral part of efforts to strengthen the country's defense preparedness in dealing with cyber warfare threats. This is in line with the Role theory put forward by Ralph Linton (1936), every individual who occupies a status in an organization has a set of roles, rights, obligations, and expectations that must be carried out consistently. In the context of the Air Force, cyber personnel occupy a strategic status as the front line in maintaining the security of defense information systems. This status demands a professional role that not only focuses on network technical security, but also on mastering the concept of cyber warfare as part of an integrated military operation.

The results of the study show that in general, Satsiberau personnel have been able to carry out the basic role of information system security, such as network monitoring, general attack mitigation, and sensitive data protection (Yudi, 2025). However, from the perspective of role theory, the demands of the role of cyber personnel in the era of cyber warfare are no longer limited to technical functions, but include cyber intelligence capabilities, advanced threat analysis, and the integration of cyber defense with military operations. The gap between role expectations and role realization is still visible, especially in the mastery of advanced techniques such as cyber threat intelligence, malware analysis, and dark web monitoring (Makmur, 2025).

Based on the view of McClelland's (1973) Competency theory, the competence of cyber personnel is a key factor in maintaining the resilience of defense information systems. The results of the study show that basic knowledge of information security, encryption, and digital intelligence data management is already possessed by most personnel. This is reflected in the participation of personnel in education such as Cyber Suspa, Cyber Susba, and cyber defence training programs. However, education that emphasizes mastery of the concepts of cyber warfare, cyber intelligence, and integrated cyber operations is still limited in number of participants (Theodorus, 2025).

In terms of skills, the possession of certifications such as CEH, CND, CPENT, and JPT shows that there is a mastery of practical skills in the field of cybersecurity, but the number of advanced certified personnel is still relatively limited. According to Evans (2008), professionalism includes not only technical skills, but also integrity, dedication, and commitment to work quality standards. In this case, the professionalism of cyber personnel is reflected in compliance with information security procedures and the implementation of SNI in the information security management system (Damanik et al., 2023).

Mejias and Balthazard (2014) emphasized that information security is not only a

technological problem, but also a human and organizational problem. In the context of the Indonesian Air Force, although the information security system has been implemented, its effectiveness depends heavily on the quality of cyber human resources. The results of the study show that the limitation of personnel with specific expertise, differences in the level of competence between individuals, and the limitation of supporting devices are the main obstacles in maintaining optimal information security. This condition has the potential to weaken the Confidentiality, Integrity, and Availability (CIA) aspects of defense information systems. In line with the High Reliability Organization framework (Weick & Sutcliffe, 2007), military organizations in the cyber era are required to have a collective capacity to detect and respond appropriately to disturbances.

Cyber Personnel Recruitment Pattern Analysis

The recruitment of TNI AU cyber personnel is the initial stage that determines the quality and readiness of human resources in dealing with cyber warfare threats. However, the results of the study show that the current recruitment pattern still follows the general soldier recruitment system with an emphasis on uniform physical requirements, age, and personal condition. Waasintel Kasau Yudi (2025) emphasized that although the need for cyber personnel with special skills has been recognized, the recruitment mechanism has not been fully adjusted to attract cyber practitioners from information technology professional backgrounds, so the fulfillment of cyber human resources is still highly dependent on general post-recruitment internal coaching. This view is strengthened by Paban VI Sandi and Siber Sintelau Makmur (2025) and Wadansatsiberau Theodorus (2025).

If analyzed through Role Theory (Linton, 1936), this condition shows a mismatch between the status and the expected role of cyber personnel. In the general recruitment system, individuals are recruited to carry out the role of soldiers with the demands of uniform physical and administrative standards. In fact, in the context of cyber warfare, cyber personnel assume new roles as technology specialists, digital intelligence analysts, and protectors of information infrastructure. According to Competency theory (McClelland, 1973), the current recruitment pattern is also not fully oriented towards mastering the core competencies of the cyber field since the initial selection stage. From the perspective of Information Security Theory (Mejias & Balthazard, 2014), the limitations of this recruitment pattern have direct implications for the effectiveness of the TNI Air Force information security system because the risk of human vulnerability is higher.

The ideal cyber personnel recruitment pattern for the Air Force must prioritize an approach based on technical competence and cyber professionalism. Recruitment needs to open a special pathway for cyber practitioners with assessments on track record, expertise certification, and technical capabilities relevant to cyber warfare threats. Aspects of military discipline are maintained, but physical and administrative requirements are no longer the dominant factors. Strategies for realizing adaptive recruitment include: 1) Establishment of cyber-specific recruitment pathways; 2) Relaxation of certain administrative requirements; 3) Establishment of clear cyber competency standards; 4) Strengthening cooperation with universities and cyber

communities; 5) Partnerships with the cybersecurity industry; 6) Development of cyber intelligence career paths; 7) Status transfer programs for civilian IT practitioners; and 8) Provision of attractive career incentives.

CONCLUSION

Strengthening the readiness of Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) personnel to address cyber warfare threats required a comprehensive strategy integrating technical capacity development and improvements to the recruitment system. This study concluded that TNI AU cybersecurity personnel had generally demonstrated basic operational competencies in mitigating common cyberattacks and protecting vital information infrastructure. However, advanced capabilities in specialized areas, including cyber threat intelligence, malware analysis, and digital forensics, remained limited. These limitations were associated with the lack of a structured specialist training curriculum and frequent personnel rotations, which hindered the continuity of competency development and the accumulation of technical expertise.

Furthermore, conventional military recruitment practices, which primarily emphasized general military selection criteria and physical requirements, presented challenges in attracting personnel with specialized cybersecurity expertise. This situation contributed to a limited supply of qualified cybersecurity professionals within the organization. Therefore, this study recommended that the Indonesian Air Force establish a specialized cybersecurity recruitment pathway based on technical competency assessments and recognized professional certifications, supported by appropriate adjustments to administrative selection requirements. It also recommended developing a structured, tiered cybersecurity education and training curriculum ranging from basic to advanced levels, facilitating access to internationally recognized professional certifications, and expanding strategic partnerships with the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN), universities, and the cybersecurity industry. These measures were expected to strengthen personnel competencies, improve institutional cyber resilience, and support the sustainable development of Indonesia's national air defense capabilities.

FUNDING

The authors declare that no financial support was received for the conduct of this study and/or the publication of this article.

CONFLICT OF INTEREST

The authors declare that this study was conducted without any commercial or financial relationships that could be interpreted as a potential conflict of interest.

AUTHORS' CONTRIBUTIONS

Indra Paulus 1: research conceptualization, methodology design, experiment execution, data collection, data analysis, manuscript drafting, and manuscript revision. Usni Hasanudin 2: research supervision, validation of research results, provision of scientific input, and manuscript review and revision. All authors have read and approved the final version of the manuscript.

STATEMENT ON THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE

The authors declare that generative artificial intelligence (AI) was used in the preparation of this manuscript to help improve linguistic clarity, correct grammar, and refine

the writing structure. Generative AI was not used to generate, manipulate, or analyze research data. The entire content of the manuscript has been reviewed and verified by the author(s). The author(s) are fully responsible for the accuracy, integrity, and final content of the manuscript.

REFERENCES

Flor-Unda, O., Puga, D., Alomoto, H., & Eguez, G. (2025). *Evolution of technology for national security: Advances and contributions of artificial intelligence*.

Castells, M. (2010). *The rise of the network society* (2nd ed., Vol. 1). Wiley-Blackwell.

Damanik, R., Andika, P., & Rahmayanti. (2023). Sistem pengamanan jaringan terhadap serangan cyber warfare [Network security system against cyber warfare attacks]. *Jurnal TNI Angkatan Udara*, *2*(2). https://e-jurnal.tni-au.mil.id/index.php/jpb/article/download/67/63

Evans, L. (2008). Professionalism, professionality and the development of education professionals. *British Journal of Educational Studies*, *56*(1), 20–38. https://doi.org/10.1111/j.1467-8527.2007.00392.x

Firdini, Gultom, R. A. G., Widodo, P., & Jupriyanto. (2024). The urgency of stakeholder cyberspace collaboration to support Indonesia's national defense. *Jurnal Perencanaan Pembangunan: The Indonesian Journal of Development Planning*, *8*(2), 150–180. https://doi.org/10.36574/jpp.v8i2.566

Guterres, A. (2018, September 24). *Address to the General Assembly* [Speech]. United Nations. https://www.un.org/sg/en/content/sg/speeches

Hardiyanto, B., & Yosepha, S. Y. (2025). Human resource development strategy at Muljono Air Base in facing data security challenges in the era of technology 5.0. *Dinasti International Journal of Management Science*, *6*(6). https://doi.org/10.38035/dijms.v6i6.5386

Laksono, A. N., Duarte, E. P., & Hendarwoto, Y. (2026). Improving the capacity of human resources in cybersecurity to support defense diplomacy in the digital era. *Jurnal Perencanaan Pembangunan: The Indonesian Journal of Development Planning*, *10*(2), 197–213. https://doi.org/10.36574/jpp.v10i2.787

Law of the Republic of Indonesia Number 3 of 2002 concerning State Defense. (2002). Statute Book of the Republic of Indonesia Year 2002 Number 3.

Linton, R. (1936). *The study of man: An introduction*. D. Appleton-Century.

McClelland, D. C. (1973). Testing for competence rather than for "intelligence." *American Psychologist*, *28*(1), 1–14. https://doi.org/10.1037/h0034092

Mejias, R. J., & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security*, *10*(4), 160–185. https://doi.org/10.1080/15536548.2014.974407

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, *136*, Article 103585. https://doi.org/10.1016/j.cose.2023.103585

Sarjito, A. (2024). Formation of the TNI Cyber Force: A strategic and policy analysis. *Defense and Security Studies*, *5*(2). https://doi.org/10.37868/dss.v5.id272

Satori, D., & Komariah, A. (2020). *Metodologi penelitian kualitatif* [Qualitative research methodology]. Rajawali Press.

Schwab, K. (2017). *The fourth industrial revolution*. Crown Business.

Sugiyono. (2014). *Metode penelitian kuantitatif, kualitatif, dan R&D* [Quantitative, qualitative, and R&D research methods]. Alfabeta.

Sutomo, A., Thamrin, S., Widodo, P., & Reksoprodjo, Y. (2025). Membangun ketahanan digital: Pengembangan model strategi pertahanan siber berbasis manajemen risiko

[Building digital resilience: Developing a risk management-based cyber defense strategy model]. *Temali: Jurnal Pembangunan Sosial*, *8*(1), 29–40. https://doi.org/10.15575/jt.v8i1.38690

Triharto, S., Pratama, R., & Dikatama, T. (2024). Pengamanan data sistem informasi Disinfolahtaau [Information system data security at Disinfolahtaau]. *Jurnal TNI Angkatan Udara*, *2*(1). https://e-jurnal.tni-au.mil.id/index.php/jpb/article/download/55/52

U.S. Department of Defense. (2023). *DoD cyber workforce strategy 2023–2027*. https://apps.dtic.mil/sti/trecms/pdf/AD1202872.pdf

U.S. Government Accountability Office. (2022). *Military cyber personnel: Opportunities exist to improve service obligation guidance and data tracking* (GAO-23-105423). https://www.gao.gov/products/gao-23-105423

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.