Journal of World Science
Vol. 5, No. 11, November 2026, pp 906-922
E-ISSN: 2828-9307
https://doi.org/10.58344/jws.v5i11.1719

Analysis of The Air Force's Cyber Resilience Readiness in Facing Cyber Warfare Threats

Taufik Hidayat*, Asep Setiawan, Asep Kurnia
Universitas Muhammadiyah Jakarta, Indonesia
Email: kifuat808@gmail.com*, Asepsetia@gmail.com, asepkurnia1109@gmail.com

Keywords:
Cyber Resilience; Cyber Warfare; Cyber Education and Training; Cyber Community

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

Copyright © 2026 by Author. Published by Riviera Publishing

ABSTRACT

Cyber warfare threatens operational continuity and information security in technology-dependent defence organisations. This study examines the Indonesian Air Force's readiness to respond to cyber threats, focusing on education and training, personnel capability, and cooperation with external cyber communities. A qualitative case-study approach was applied to the Air Force Cyber Unit (Satsiberau), drawing on purposively selected institutional and community informants, interviews, participatory observation, policy documents, and the incident records presented in the manuscript. Findings show that established training pathways provide essential entry-level competencies but have not fully kept pace with advanced threat scenarios. Constraints include uneven specialist skills, limited simulation facilities and instructor capacity, short course durations, and weak integration between training assessment and operational feedback. Incident records show one reported incident in 2022, eight in 2023, eighteen in 2024, and eight in 2025, but these counts alone cannot establish changes in readiness or exposure. External cyber communities contribute vulnerability information and informal early warning; however, collaboration depends largely on personal networks and lacks consistent verification, feedback, and institutional safeguards. The study proposes adaptive tiered training, realistic incident exercises, and controlled two-way community engagement. Because the evidence is qualitative and case-specific, operational effectiveness of the proposed measures requires further assessment.

INTRODUCTION

Digital transformation has increased the dependence of defense organizations on interconnected information systems, cloud-based services, and data-driven decision-making processes (Abedalrhman & Alzaydi, 2026). This growing dependence has exposed military operations to cybersecurity threats, including system disruptions, unauthorized access to sensitive information, and cyberattacks that may compromise the confidentiality, integrity, and availability of critical information assets. Consequently, national security research has increasingly conceptualized cyber resilience as a multidimensional organizational capability encompassing preparedness, threat detection, incident response, operational continuity, and recovery rather than merely a technical security measure (Candra et al., 2021; Hadi et al., 2025; Sutomo et al., 2025; Vimy et al., 2022).

Cybersecurity incidents affecting critical infrastructure have demonstrated the importance of organizational preparedness, coordinated incident response, and operational continuity planning. Reported disruptions involving aviation service systems in Europe in 2025, alongside subsequent cybersecurity allegations involving Germany, illustrated the potential vulnerability of strategically important infrastructure to cyber threats (Reuters, 2025a, 2025b). Although these incidents did not provide direct evidence of cybersecurity vulnerabilities within the Indonesian Air Force, they highlighted the broader operational risks associated with increasingly interconnected digital systems. Such developments emphasized the need for qualified cybersecurity personnel capable of detecting anomalous activities, coordinating incident responses, mitigating operational disruptions, and restoring essential functions while maintaining information security.

The Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) faces particular cybersecurity challenges because military aviation operations depend on interconnected digital infrastructure, reliable information systems, and specialized technical personnel. Indonesia's national defense framework provides a legal foundation for mobilizing human resources, technological capabilities, and institutional support to strengthen national defense preparedness (Republic of Indonesia, 2002). Within this organizational context, the Indonesian Air Force Cyber Unit (Satuan Siber TNI Angkatan Udara, Satsiberau) performs cybersecurity monitoring and incident response functions, while military education and training institutions contribute to personnel competency development. However, the effectiveness of cyber resilience depends not only on the availability of formal policies and training programs but also on their integration with operational requirements, institutional coordination, and continuous professional development.

Institutional records documented one cybersecurity incident in 2022, eight in 2023, eighteen in 2024, and eight in 2025. These figures, presented in the cybersecurity monitoring dashboard in Figure 1 and summarized in Table 1, indicated fluctuations in recorded cybersecurity incidents rather than a consistent increase throughout the observation period. Furthermore, incident counts alone could not establish changes in cyber threat severity, monitoring effectiveness, organizational vulnerability, or incident recovery capabilities. Nevertheless, the documented incidents provided an empirical basis for examining whether existing cybersecurity education and training programs adequately prepared personnel to address diverse and increasingly complex operational threats. The variation in reported incidents also highlighted the importance of assessing personnel readiness, incident response coordination, and the capacity to translate cybersecurity knowledge into operational practice.

Previous studies have examined several dimensions of cybersecurity personnel development and military cyber preparedness. Shin et al. (2024) and Park et al. (2022) emphasized the contribution of continuous professional training and cyber range-based exercises to strengthening cybersecurity competencies and incident response capabilities. Meanwhile, Kurniawan and Prasojo (2022) investigated broader dimensions of military cybersecurity competence, highlighting the importance of personnel capabilities in supporting institutional preparedness. Although these studies provided valuable insights into cybersecurity education, training effectiveness, and professional competency development, they did not comprehensively explain how training evaluation, specialist personnel retention, operational feedback, and collaboration with external cybersecurity communities were integrated within

Satsiberau. A comparison of the relevant studies is presented in Table 2, highlighting the remaining conceptual and empirical limitations in understanding the relationship between formal institutional preparedness and external cybersecurity collaboration.

The principal research gap concerned the limited empirical understanding of how cybersecurity education and training systems interacted with external cybersecurity communities to strengthen the Indonesian Air Force's organizational readiness against cyber warfare threats. This gap was particularly important because formal competency development programs and community-generated vulnerability intelligence might operate independently without effective mechanisms for verification, institutional coordination, and operational integration. The study's novelty lay in its integrated examination of discrepancies between cybersecurity training policies and operational practices, alongside the institutional governance of community-sourced vulnerability information and early warning contributions. By examining these interconnected dimensions, the research sought to identify organizational constraints and opportunities for strengthening cybersecurity preparedness through adaptive personnel development and structured external collaboration. However, the study did not attempt to quantify overall institutional cyber resilience or establish the causal effectiveness of specific cybersecurity interventions. Instead, it provided a qualitative assessment of institutional readiness and a basis for developing context-sensitive recommendations to strengthen the Indonesian Air Force's cyber resilience against evolving cyber warfare threats.



Figure 1. Satsiberau Threat Anomaly Monitoring Dashboard
Source: Satsiberau monitoring material reproduced in the original manuscript

Table 1. Cyber Incidents in the Indonesian Air Force in 2022 to 2025

Time	Number of Cyber Incidents	Types of Cyberattacks
Year 2022	1	*Sensitive Data Exposure*
Year 2023	8	*Sensitive Data Exposure*, *Web Defacement*, *Cross Site Scripting*
Year 2024	18	*Web Defacement*, *Sensitive Data Exposure*, *SQL Injection*
Year 2025	8	*Web Defacement*, *Sensitive Data Exposure*, *Ransomware*

Source: Cyber incident records presented in the original manuscript (2022–2025).

This study aimed to examine the contribution of cybersecurity education and training to personnel readiness, identify operational and organizational constraints affecting cyber resilience, and explore opportunities for secure collaboration with external cybersecurity communities. Conceptually, the study integrated organizational resilience theory and the communities of practice perspective to provide a comprehensive, case-based understanding of cybersecurity preparedness within the Indonesian Air Force (Weick & Sutcliffe, 2007; Wenger, 1998). From a practical perspective, the findings were intended to inform the development of adaptive cybersecurity training curricula, realistic cyber incident simulation exercises, specialized personnel competencies, and institutional governance mechanisms for receiving, verifying, and responding to externally reported cybersecurity vulnerabilities while safeguarding sensitive military information.

Table 2. Summary of Previous Research

Researcher	Focus and Key Findings	Differences with This Study
Romadhon & Salman (2025)	Development of cyberattack scenarios for local government TTIS training	Not only the technical scenario, but also the role of the cyber community
Toth et al. (2025)	Continuous phishing training improves threat identification	Wider coverage: conceptual, technical, and community networking
Kusuma et al. (2024)	The challenge of increasing the capabilities of military personnel in the face of cyber threats	Includes the role of a cyber community network
Sarjito (2024)	Evaluation of the formation of the TNI Cyber Force; HR, technology, and coordination constraints	Focus on education, training, and cyber community
Shin et al. (2024)	Cyber range and integrated training scenarios improve personnel response	Specific to the Indonesian Air Force and the role of the cyber community
Fernandes & Abosata (2024)	India's *cyber warfare* readiness and education strengthening needs	Discussing the role of cyber communities
Alamin et al. (2023)	Cybersecurity training for East Java Police members	Also examine the use of cyber communities
Kurniawan & Prasojo (2022)	Conceptual framework of cyber competence of military personnel	Includes technical readiness and community networking
O'Neill et al. (2021)	Scenario-based training framework for cyber incident handling	Also examine the role of the cyber community

Source: Author's synthesis of the studies cited in this manuscript.

METHOD

This study employed a qualitative descriptive-analytical case study design focusing on the Indonesian Air Force Cyber Unit (Satuan Siber TNI Angkatan Udara, Satsiberau), its personnel development programs, and collaboration with external cybersecurity communities. The research was conducted from October 2025 to February 2026 and examined cybersecurity policy implementation, incident response preparedness, specialized personnel competencies, and institutional collaboration mechanisms. Informants were selected through purposive sampling based on their experience in military command, cybersecurity training, information security, and community engagement. Participants included senior Indonesian Air Force representatives, cybersecurity unit personnel, training officials, and two external cybersecurity community representatives whose identities were anonymized. The informant categories are presented in Table 3.

Data were collected through semi-structured interviews, participant observation, document analysis, and reviews of available cybersecurity incident records. Interviews explored training curriculum relevance, training frequency, infrastructure availability, instructor competencies, operational performance evaluation, information-sharing practices, and barriers to institutional collaboration. The researcher's previous involvement with Satsiberau facilitated contextual understanding and access to relevant information, while potential researcher bias was addressed through reflexive interpretation and comparison of evidence from multiple sources. Data credibility was strengthened through triangulation of interview findings, observational evidence, institutional documents, and perspectives from different informant groups. The collected data were analyzed descriptively and thematically to identify recurring patterns, institutional constraints, and opportunities for improving cybersecurity personnel readiness and collaboration with external cybersecurity communities.

Table 3. Research Informant

Yes	Informants	Role
1	Deputy Intelligence Assistant to the Chief of Staff of the Air Force (Waasintel Kar)	Supervision of operational and cyber activities of the Indonesian Air Force
2	Paban VI Sandi and Siber Sintelau	Formulation of intelligence and information security policies of the Indonesian Air Force, including the direction of strengthening *cyber resilience*
3	Commander of the Indonesian Air Force Cyber Unit (Dansatsiberau)	Person in charge of cyber security management, incident handling, and cyber personnel coaching
4	Commander of the 506th Squadron of Education 500 (506th Infantry)	Implementation of cyber education and training as well as the formation of cyber personnel competencies
5	Cyber Community (2 people, initials A and B)	External cyber practitioners; identities kept confidential for confidentiality and security

Source: Informant roster presented in the original manuscript.

Data were analyzed using the interactive model of Miles et al. (2014), comprising data reduction, thematic data display, and conclusion drawing and verification. Source triangulation was conducted by comparing interview findings, observational data, and institutional documents to strengthen the credibility of the analysis. Thematic analysis focused on

cybersecurity education and training, personnel readiness, and contributions from external cybersecurity communities. Existing institutional practices were compared with operational readiness requirements identified by informants to determine recurring challenges and opportunities for improvement. The analytical process is illustrated in Figure 2. Findings were interpreted within the specific organizational context of the Indonesian Air Force Cyber Unit, recognizing that reported cybersecurity incident counts did not independently establish organizational readiness and that community-generated information required appropriate confidentiality safeguards. Accordingly, the proposed recommendations were treated as potential institutional improvements requiring further operational evaluation rather than empirically demonstrated causal effects.

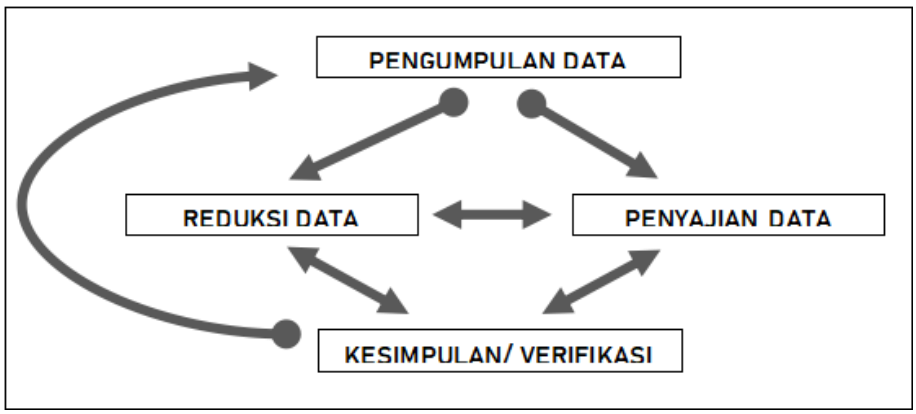


Figure 2. Miles et al. Model Data Analysis Techniques

Source: Miles et al. (2014), as illustrated in the original manuscript.

RESULTS AND DISCUSSION

This research focuses on Satsiberau, which is under the Indonesian Air Force Headquarters as the Central Executive Agency (Balakpus) responsible to the Rafters for the security, monitoring, and handling of cyber incidents in all Indonesian Air Force work units. Satsiberau plays a role as the forefront of air defense in maintaining the *confidentiality*, *integrity*, and *availability of the* Indonesian Air Force information system, as well as a node for fostering cyber personnel capabilities and developing information security procedures.

In general, the readiness of the Indonesian Air Force cyber human resources shows that there are institutional efforts in developing cyber capabilities through the recruitment of personnel with information technology backgrounds, cyber education and training, and assignments to related units. However, in terms of quantity, the number of cyber personnel is still limited compared to the breadth of the threat spectrum and workload. In terms of quality, the mastery of technical competencies has not been fully followed by a career development system, continuous certification, and adequate cyber human resource retention mechanisms, while the dynamics of general mutation and rotation of positions also affect the continuity of cyber expertise. In a cross-dimensional comparison, the TNI Headquarters tends to play the role of a policy controller and strategic coordinator, the TNI AD excels in the quantity of human resources and the reach of territorial organizations, and the TNI Navy is oriented towards the protection of weapons systems and maritime C4ISR. The Indonesian Air Force has advantages in the high level of technology adoption and the dependence of the air operating system on

digital networks, but still faces a limited number of cyber human resources, the sustainability of competency development, and the integration of cyber roles in the air defense system. This condition puts the readiness of the Indonesian Air Force cyber human resources at a developing stage.

Cyber Education and Training in Personnel Competency Formation

Cyber Education and Training Policy Direction

The direction of the TNI Air Force's cyber education and training policy is part of the national policy chain. The President sets the direction of defense policy reflected in the Defense White Paper, which explicitly includes cyber threats as one of the strategic threats to the country's sovereignty and security. The TNI Commander then conveyed the policy direction to the Chief of Staff of the Forces, including the Rafters, so that the Rafter's policy on cyber education and training is a direct implementation of national policies and the policies of the TNI Commander. This is in line with defense policy theory, which emphasizes the alignment of military, institutional, and human resource capabilities with the character of threats. Waasintel Kasau emphasized that "*cyber warfare* cannot be seen only as a technical disturbance, but as a strategic threat that can affect operational preparedness and the stability of the country's defense" (Yudi, personal communication, 2025). At the operational level, Dansatsiberau stated that "cyber personnel must be able to maintain the continuity of systems that support operations, because cyber disturbances can have a direct impact on the implementation of TNI AU's duties" (Ketut, personal communication, 2025).

This view is in line with the Theory of Organizational Resilience (Weick & Sutcliffe, 2007), especially the principles *of preoccupation with failure*, *sensitivity to operations*, and *commitment to resilience*, which emphasizes the importance of early awareness of potential disruptions in high-risk organizations. Cyber education and training are not positioned simply as a 912he author of competency administration, but as operational provisions that determine the sustainability of information systems and networks that support the main tasks of the unit. However, Danskadik 506 acknowledges that "we strive to ensure that educational materials are relevant to the needs of the unit, but there are still limitations in reaching the development of highly dynamic cyber threats" (Rizan, personal communication, 2025). These findings show that policy direction is clear and aligned between the strategic, operational, and educational levels, but there is still a gap between *the commitment to resilience* at the policy level and the institutional ability to realize it operationally.

Cyber Education and Training Curriculum

Paban VI Sandi and Siber Sintelau emphasized that "cyber threats are very dynamic and continue to evolve, so the cyber education curriculum should ideally not be static, but updated periodically to align with the actual threat pattern and its potential strategic escalation" (Makmur, personal communication, 2025). Dansatsiberau assessed that "the existing curriculum has provided a sufficient basis, but when dealing with dynamic and complex cyber threats, personnel still have to relearn a lot through operational experience" (Ketut, personal communication, 2025). Danskadik 506 explained that curriculum adjustments are carried out gradually through evaluation and unit input, "but the limited time, instructors, and means make the material still emphasize more basic mastery, while the latest threats are only given at the

introductory stage" (Rizan, personal communication, 2025). The list of cyber education organized by Skadik 506/Wingdik 500 in the 2025 Fiscal Year is presented in Table 4.

Table 4. List of Education in Skadik 506/Wingdik 500

Yes	Education Name	Number of Students				Dik Time
		PA	TO	PLOT	PNS	
1	1st Cybersecurity Basics Course	6	22	21	-	3 months
2	33rd Computer Operator Course	-	7	10	-	2 months
3	27th Lek Vocational Management (IT) Course	-	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
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

The implementation of education is based on a number of Rafter decisions on the cyber education curriculum as presented in Table 5.

Table 5. Basic Curriculum of Cyber Education Skadik 506/Wingdik 500

Yes	Rafter Decision	About
1	Kep/269/IX/2024	Cybersecurity Basic Course Education Curriculum
2	Kep/273/IX/2024	Suspa Cybersecurity Management Education Curriculum
3	Kep/270/IX/2024	Junior Education Curriculum Penetration Testing
4	Kep/272/IX/2024	Forensic Digital Education Curriculum
5	Kep/271/IX/2024	LV1 Security Operation Center Analyst Education Curriculum
6	Kep/26/II/2025	TNI AU Cyber Branch Education Curriculum

Source: Skadik 506/Wingdik 500, as reported in the manuscript.

The Skadik 506 curriculum includes an introduction to cybersecurity concepts, the basics of securing networks and information systems, ICT infrastructure management, an introduction

to the types of cyber threats, and the formation of professional attitudes and information security disciplines. This curriculum serves as an *entry-level capability* that prepares personnel before entering the operational environment. However, when faced with dynamic and complex threats such as *ransomware*, data leaks, and layered attacks on IIVs, educational materials do not fully reflect real operational conditions. This is not in line with the principle of *reluctance to simplify interpretations* (Weick & Sutcliffe, 2007) which emphasizes understanding the complexity of threats without excessive reduction. As a result, many personnel still have to develop advanced capacity through operational experience, rather than through structured education pathways, so there is a gap between the operational capability demands of cyber units and the available curriculum capacity.

The Role of Education and Training in Supporting Technical Competence

Paban VI Sandi and Siber Sintelau stated that "technical competence is the main prerequisite in supporting the cyber intelligence function, especially in information technology-based threat collection, analysis, and mitigation. Without adequate technical competence, cyber intelligence capabilities will not be optimal in providing early warning and strategic recommendations" (Makmur, personal communication, 2025). Dansatsiberau added that "the technical competence of personnel is formed through a combination of formal education and direct practice. However, not all personnel have the same level of competence, so education and training need to be designed in more stages" (Ketut, personal communication, 2025). Differences in educational backgrounds, variations in assignment intensity, and limited opportunities to participate in advanced training cause technical abilities between personnel to be not equal.

The researcher's observation found that as many as 17 Satsiberau personnel have international and national standard cyber certifications that are relevant to Satsiberau's duties. Skadik 506 also collaborates with the State Cyber and Cryptography Agency (BSSN) in the implementation of certifications for students after completing education, namely the certification of Information Security Security Auditor Assistant after the Cybersecurity Management Officer Course, as well as the certification of Junior Penetration Tester, Lv1 Security Operation Center Analyst, and Digital Forensic after related courses. However, Danskadik 506 stated that "the limitations of simulation facilities and budgets make real-scenario based practices not optimal, so graduates still need further reinforcement in the unit" (Rizan, personal communication, 2025). Thus, cyber education and training have been designed to form technical competencies gradually, but the implementation still focuses on basic technical competencies so that it has not fully answered the needs of advanced technical capabilities demanded by the dynamics of *cyber warfare* threats.

The Role of Cyber Training in Improving Personnel Response

Waasintel Kasau emphasized that "from an intelligence perspective, the speed and accuracy of responses are key factors to prevent the escalation of threats and the leakage of strategic information. Therefore, cyber exercises must be able to form the operational reflexes of personnel" (Yudi, personal communication, 2025). Dansatsiberau said that "cyber exercises have helped increase the basic readiness of personnel in responding to incidents. However, in complex and continuous incidents, personnel still need a long adaptation time. In addition, only a few personnel can take part in cyber exercises due to the limited number of personnel who master the technicals" (Ketut, personal communication, 2025). Several Satsiberau personnel

have participated in cyber exercises, both as actors and organizers, within the TNI and with other countries, as presented in Table 6.

Table 6. List of Cyber Training of Satsiberau Personnel

Yes	Exercise Name	Engagement
1	Super Bowl (2023–2024)	4 personnel as perpetrators
2	Cobra Gold Cyber Exercise (2023)	1 personnel as perpetrators
3	Indus Shield Cyber Exercise (2024)	1 personnel as perpetrators
4	Cyber Exercise (2024)	1 personnel as perpetrators
5	Air Force Cyber Defence Exercise (2021–2025)	4 actors, 4 organizers
6	Cyber Training at the Yudha Space Exercise (2021–2025)	2 actors, 2 organizers

Source: Training records presented in the original manuscript.

In the perspective of Weick and Sutcliffe (2007), cyber training functions as a mechanism to build *sensitivity to operations* and *commitment to resilience*. The findings show that cyber training has contributed to building basic readiness of personnel in simple disruption scenarios, but has not fully trained personnel to face *unexpected events* that are *non-linear*, ambiguous, time-pressured, and require quick decisions based on incomplete information. From the perspective of human resource theory, the limited number of personnel with deep technical mastery causes the participation of the exercise to be uneven, so that the improvement of response capabilities is centered on certain groups of personnel. Danskadik 506 also states that "operational training in education is still limited by facilities and time. As a result, the simulations conducted have not fully reflected the dynamics of cyber incidents in the field" (Rizan, personal communication, 2025). In the perspective *of Transformative Learning* (Mezirow, 1991), real-world scenario-based training acts as a *disorienting dilemma* that encourages critical reflection and a change in ways of thinking; when the training is still limited and less contextual, the adaptability and decision-making of personnel only develops after facing real incidents in the field.

Cyber Education and Training Challenges and Evaluations

The challenges of implementing cyber education and training are multidimensional. At the policy level, Paban VI Sandi and Siber Sintelau stated that "the main challenge lies in the gap between the increasingly complex cyber defense needs and the availability of competent and equitable cyber human resources. Cyber threats are developing rapidly, while the process of forming military human resources requires time, discipline, and a structured system" (Makmur, personal communication, 2025). At the unit level, Dansatsiberau highlighted "the limited number of cyber personnel with in-depth expertise, especially in specific areas such as advanced *incident response* and threat analysis. The complexity of the threats faced often goes beyond formal education scenarios" (Ketut, personal communication, 2025). At the level of education providers, the main challenge relates to "the limitation of instructors who have adequate certification and practical experience, as well as simulation facilities that have not fully supported training based on real threat scenarios" (Rizan, personal communication, 2025).

The evaluation mechanism for the effectiveness of cyber education and training has been implemented at various levels, but it is still partial. At the strategic level, the evaluation is carried out by looking at the contribution of education and training to cyber intelligence

preparedness and early detection capabilities (Makmur, personal communication, 2025). At the unit level, effectiveness is assessed from the ability of personnel to respond to incidents quickly, precisely, and measurably, "but this evaluation is still internal and has not been fully integrated with the formal education assessment system" (Ketut, personal communication, 2025). Meanwhile, evaluations in educational institutions "focus more on students' academic achievements", so the link between educational outcomes and graduate performance in operational units needs to be strengthened through a more systematic feedback mechanism (Rizan, personal communication, 2025). In the perspective *of Communities of Practice* (Wenger, 1998), this condition shows that collective learning between operational units and educational institutions has not been optimally connected, so tacit knowledge from the field has not been transformed into institutional knowledge. It also shows that the learning process is not fully reflective and transformative as emphasized by Mezirow (1991).

Ideal Framework and Steps to Improve the Quality of Cyber Education and Training

Waasintel Kasau stated that "in the future, TNI AU cyber education and training need to be developed strategically and adaptively, in line with the dynamics of global threats and national defense interests", including "aligning the curriculum with actual threat maps and strengthening the role of cyber intelligence as an *early warning system*" (Yudi, personal communication, 2025). In terms of graduate users, Dansatsiberau emphasized that the ideal direction of development is "increasing personnel specialization and organizing exercises based on real scenarios, so that units have an adequate depth of competence", as well as a curriculum that "equips personnel with multi-level abilities and encourages *problem solving* and decision-making" (Ketut, personal communication, 2025). Cyber personnel need to be equipped with advanced competencies according to their specific tasks, such as *advanced incident response*, cyber threat analysis, digital forensics, and securing vital information infrastructure. Paban VI Sandi and Siber Sintelau added that strengthening the curriculum needs to integrate technical, conceptual, and strategic aspects (Makmur, personal communication, 2025), while Danskadik 506 emphasizes regular curriculum updates, improving the quality of instructors, as well as "a combination of classical learning, laboratory practice, and real-case simulation" (Rizan, personal communication, 2025).

In Mezirow's (1991) perspective, cyber education ideally does not only transfer technical knowledge, but encourages a change in personnel's mindset from reactive to anticipatory, reflective, and adaptive. In line with the concept of *Communities of Practice* (Wenger, 1998), simulations and exercises based on real scenarios function as a collective learning medium that allows students to internalize knowledge that develops in the operational environment. Thus, the strengthening of TNI AU cyber education and training needs to be carried out comprehensively through curriculum alignment with threat maps, specialization development, improvement of instructor quality, development of realistic simulations, and sustainable policy and budget support.

The Role of the Cyber Community in Supporting Personnel Professionalism

Functions of Cyber Community

The development of cyber communities by the Indonesian Air Force is a strategic response in involving the community as part of Sishankamrata. Within the framework of defense policy theory, defense policy requires the integration of all national components,

including the cyber community, in order to respond to the development of threat characteristics that are cross-sectoral, asymmetrical, and non-conventional. Waasintel Kasau stated that "the cyber community has a role as a space for consolidating knowledge and perception of cyber threats that are increasingly complex and multidimensional, as well as helping to equalize the perspective of *cyber warfare* as a strategic threat" (Yudi, personal communication, 2025). Dansatsiberau added that "through cyber communities, personnel can gain practical lessons from real cases, so it is very helpful in increasing awareness and quality of response to cyber incidents" (Ketut, personal communication, 2025).

The external cyber community has a unique function that cannot always be fulfilled by a formal coaching system. Cyber Community A explains that the external community is "a pool of non-conventional talent that the formal recruitment system of the Indonesian Air Force may not be able to reach, such as self-taught methods, *neurodivergents* or individuals with atypical career paths but have exceptional technical expertise", so that relations with the community open access to *diversity of thought* that is difficult to produce internally in hierarchical institutions (Cyber Community A, 2025). Cyber Community B affirms that the external community plays a role "as a source of technical intelligence and early detection of cyber threat dynamics" through monitoring, vulnerability research, and incident analysis, as well as a collective learning space to share best practices and mitigation techniques (Cyber Community B, 2025). These findings are in line with the principles *of preoccupation with failure* and *reluctance to simplify* within the framework *of High Reliability Organizations* (Weick & Sutcliffe, 2007) and the concept *of Communities of Practice* (Wenger, 1998), where knowledge is constructed through real practice and *tacit knowledge exchange*. Cyber communities have the potential to become *knowledge hubs* that complement formal education renewal cycles that are slower than the speed of cyber threat evolution.

Cyber Community Engagement and Relationship Patterns with Satsiberau

The external cyber community's contribution is voluntary and focuses on the initial delivery of information. Cyber Community A explained that the main form of contribution is "system vulnerability reporting" which is submitted voluntarily as a form of concern for national security, and some government organizations respond well to it so that communication channels are formed (Cyber Community A, 2025). Cyber Community B states that the information conveyed is generally related to "system vulnerabilities and data breach incidents that are traded on the *dark web*" (Cyber Community B, 2025). This shows that the external community also plays a role as a non-formal cyber intelligence actor, which in the perspective of *High Reliability Organizations* reflects the importance of *deference to expertise*, which is the recognition of the source of expertise outside the formal structure of the organization.

At the unit level, the contribution is realized through direct reports from around three to five cyber practitioners whose identities are kept secret for security reasons. Dansatsiberau stated that "this information is very valuable as an *early warning*, but because there is no official mechanism, work program, and sustainable management, the contribution is not optimal" (Ketut, personal communication, 2025). Paban VI Sandi and Siber Sintelau assessed that "the relationship pattern that has been formed today is still inadequate and patterned. The trust that emerges is individual and has not been supported by a clear organizational system or mechanism" (Makmur, personal communication, 2025). From the perspective of the community, Cyber Community A said that communication patterns were "informal, based on

personal relationships and unstructured", while Cyber Community B emphasized that the absence of formal communication channels caused the flow of information to tend to be one-way because the community "rarely received official clarifications, evaluations, or follow-ups" (Cyber Community A, 2025; Cyber Community B, 2025). In the perspective *of Communities of Practice* (Wenger, 1998), these interactions have not fulfilled the elements of community and practice in their entirety, while in the theory of Professionalism (Freidson, 2001), this condition limits the use of professional expertise from outside the organization because there is no mechanism that integrates competencies, standards of practice, and ethical responsibilities into Satsiberau's formal work system.

Barriers, Impacts, and Implications of Unmanaged Community Engagement

The main obstacle to managing external cyber communities comes from policy and strategic planning aspects. Paban VI Sandi and Siber Sintelau stated that "the main problem lies at the policy and strategic planning level, namely the lack of a regulatory framework that specifically regulates collaboration with the external cyber community, so it has not been included in the organization's work programs and budgets" (Makmur, personal communication, 2025). As a result, Satsiberau does not yet have a planning basis to prepare concrete activities such as official communication forums, routine coordination mechanisms, and the integration of community contributions into the cycle of education, training, and cyber incident response (Ketut, personal communication, 2025). In the perspective of Weick and Sutcliffe (2007), this condition shows low *sensitivity to operations* and weak *organizational learning*, because the organization has not systematically utilized external knowledge sources.

Unmanaged community involvement has strategic and operational impacts. Paban VI Sandi and Siber Sintelau stated that "this condition limits the ability of the Indonesian Air Force to build collective and sustainable cyber resilience, because information from the community has not been converted into systemic learning and preparedness" (Makmur, personal communication, 2025), so organizations tend to be reactive and focus on short-term recovery. Dansatsiberau added that "the reliance on informal relationships causes inconsistent responses and is difficult to standardize, so the potential of cyber communities as *a force multiplier* has not been optimally utilized" (Ketut, personal communication, 2025). From a network perspective, Waasintel Kasau views the external cyber community as an information node (*external nodes*) that shows that the TNI AU's cyber defense is in a broader network, "but because it has not been institutionalized, the relationship is still *ad hoc* and has not become an adaptive and resilient system" (Yudi, personal communication, 2025). Without feedback and documentation mechanisms, knowledge from the community does not become an organizational memory. This condition reflects a *low-density network*, where the flow of information is one-way, non-repetitive, and not institutionally internalized.

Challenges and Steps to Capture External Cyber Communities

Waasintel Kasau stated that "the biggest challenge is how to establish a balance between the need for openness to external cyber networks and the obligation to maintain the security and confidentiality of military information, so that collaboration can run without creating new vulnerabilities" (Yudi, personal communication, 2025). The involvement of external actors cannot be separated from the risk of information leakage, misuse of access, and the emergence of new vulnerabilities, so an adequate regulatory framework, role limitations, and control mechanisms are needed. Dansatsiberau added that "without a standard mechanism, incentive

scheme, and official forum, it is difficult for us to capture and engage more cyber communities in a sustainable manner, because relationships are still highly dependent on personal relationships" (Ketut, personal communication, 2025). In the perspective of Weick and Sutcliffe (2007), this shows the challenge in building *organizational mindfulness*, especially in managing the tension between adaptation needs and security demands.

The step to overcome these challenges is the preparation of concrete policies in the form of official work programs in the field of cyber collaboration. Waasintel Kasau emphasized the need for "the preparation of an official work program in the field of cyber collaboration that is part of the strategic planning of the Indonesian Air Force and supported by an adequate budget" (Yudi, personal communication, 2025). Dansatsiberau emphasized that the management of the cyber community needs to be carried out "systematically through official forums, information verification procedures, and follow-up mechanisms that are integrated with incident response systems" (Ketut, personal communication, 2025). This step requires a paradigm shift from a purely institutional command approach to network-based collaboration, which translates through the prioritization of activities, safe and controlled collaborative governance, and sustainable resource allocation.

The Ideal Cyber Community Management Model

Waasintel Kasau stated that "the ideal cyber community management model is one that is selectively institutionalized and integrated into the TNI AU's cyber defense policy, and realized through an official work program supported by a budget" (Yudi, personal communication, 2025). The cyber community is positioned as *a supporting node* in the early warning system, so a policy framework is needed that regulates the objectives of involvement, the scope of contribution, the mechanism for securing sensitive information, and the limits of authority. Dansatsiberau emphasized that "with a structured two-way communication pattern and an institutional appreciation mechanism supported by work programs and budgets, cyber community networks can develop into adaptive and mutually trusting networks" (Ketut, personal communication, 2025). Through the stages of clarification, joint analysis, and evaluation, information from the community can be internalized into Satsiberau's standard procedures, doctrines, and response patterns. In network terminology, this condition reflects the formation *of a high-density network*, where interactions between nodes are repetitive, reciprocal, and oriented towards collective learning (Wenger, 1998). Thus, the ideal cyber community management model to support the cyber *resilience* of the Indonesian Air Force is an institutionalized, selective, and integrated model with organizational planning, budgeting, and learning systems.

CONCLUSION

Cybersecurity education and training within the Indonesian Air Force provided a foundation for developing specialized personnel competencies and strengthening operational preparedness. However, the findings revealed persistent gaps between the increasing complexity of cyber warfare threats and the capabilities supported by existing training programs. Major challenges included insufficient training duration, disparities in specialized cybersecurity competencies, limited simulation infrastructure and qualified instructors, and inadequate integration of training assessments with operational feedback. External cybersecurity communities contributed vulnerability intelligence and early warning

information, but institutional collaboration remained largely informal and dependent on personal networks. These findings highlighted organizational and institutional constraints affecting cybersecurity preparedness, although the qualitative evidence did not establish a direct causal relationship between the identified factors and overall cyber resilience.

Future improvements should prioritize the development of tiered, competency-based cybersecurity training curricula aligned with evolving cyber threats, the expansion of realistic cyber incident simulation exercises, and continuous professional development for specialized personnel. Training evaluations should also be systematically integrated with operational incident response assessments to strengthen the alignment between acquired competencies and practical readiness. Furthermore, collaboration with external cybersecurity communities should be institutionalized through authorized vulnerability reporting channels, standardized information verification procedures, structured feedback mechanisms, and appropriate safeguards for sensitive military information. Future research should employ longitudinal and mixed-methods approaches to evaluate the effectiveness of these measures, examine measurable indicators of incident detection, response, and recovery capabilities, and compare cybersecurity governance arrangements across relevant military institutions where security restrictions permit. Such efforts would provide stronger empirical evidence for distinguishing proposed institutional improvements from demonstrated advances in the Indonesian Air Force's cyber resilience.

FUNDING

The author(s) declared that financial support was not received for this work and/or its publication.

ACKNOWLEDGEMENTS

If any, an acknowledgment may be made here. This section displays the author's appreciation to sponsors, fund donors, resource persons, or parties who have an important role in conducting research.

CONFLICT OF INTEREST

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

AUTHOR CONTRIBUTIONS

If applicable, the Author's Contribution Statement.

GENERATIVE AI STATEMENT

The author(s) declared that generative AI was used in the creation of this manuscript. The author(s) wish to acknowledge the use of Generative AI for refining the language clarity and grammatical structure of this manuscript. This application was conducted in adherence to established ethical guidelines regarding the use and disclosure of generative AI in scholarly research. Each author has provided substantial intellectual contributions to the work, which has been rigorously vetted for accuracy, and the author(s) assume full responsibility for the integrity and final contentofthemanuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made

to ensureaccuracy, including review by 921he authors wherever possible. If you identify any issues, please contact us.

REFERENCES

Abedalrhman, K., & Alzaydi, A. (2026). Accelerating Digital Transformation: A Strategic Roadmap for Enterprises Adopting AI, Cloud Computing, and Data-driven Solutions in the Digital Era-An Analytical Study within the Syrian Context. *Cloud Computing, and Data-Driven Solutions in the Digital Era-An Analytical Study within the Syrian Context (June 05, 2026)*.

Alamin, M. M., Editya, A. S., Kurniati, N., Pramana, A. L., & Lisdiyanto, A. (2023). Peningkatan kualitas SDM melalui pelatihan cyber security pada anggota Polisi Daerah Jawa Timur. *PARTA: Jurnal Pengabdian kepada Masyarakat, 4*(2), 150–155. https://doi.org/10.38043/parta.v4i2.4655

Candra, A., Suhardi, & Persadha, P. D. (2021). Indonesia facing the threat of cyber warfare: A strategy analysis. *Jurnal Pertahanan, 7*(3), 441–451. https://doi.org/10.33172/jp.v7i3.1424

Fernandes, Y., & Abosata, N. (2024). *Analysing India's cyber warfare readiness and developing a defence strategy* (arXiv:2406.12568). arXiv. https://doi.org/10.48550/arXiv.2406.12568

Freidson, E. (2001). *Professionalism: The third logic*. University of Chicago Press.

Hadi, M. D. S., Gultom, R. A. G., Ansori, & Kustiawan, B. (2025). Defense information systems architecture for cyber threats: A systematic review of the research literature. *Jurnal Penelitian Pendidikan IPA, 11*(10), 10–22. https://doi.org/10.29303/jppipa.v11i10.12905

Kurniawan, R., & Prasojo, E. (2022). Conceptual framework for cyber competence of military institution personnel in the digital age: A literature review. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal), 5*(2), 12191–12203.

Kusuma, A. W., Zulkifli, M., Bay, A. U., Nurhartonosuro, I. M., & Muhadi, M. (2024). Meningkatkan kapabilitas personel militer dalam mengatasi ancaman dunia maya: Tantangan dan solusi. *Jurnal Pendidikan Tambusai, 8*(2), 36599–36606. https://jptam.org/index.php/jptam/article/view/19483

Mezirow, J. (1991). *Transformative dimensions of adult learning*. Jossey-Bass.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). SAGE Publications.

O'Neill, A., Ahmad, A., & Maynard, S. (2021). *Cybersecurity incident response in organisations: A meta-level framework for scenario-based training* (arXiv:2108.04996). arXiv. https://doi.org/10.48550/arXiv.2108.04996

Park, M., Lee, H., Kim, Y., Kim, K., & Shin, D. (2022). Design and implementation of multi-cyber range for cyber training and testing. *Applied Sciences, 12*(24), Article 12546. https://doi.org/10.3390/app122412546

Republic of Indonesia. (2002). *Law of the Republic of Indonesia Number 3 of 2002 concerning State Defense*.

Reuters. (2025a, September 20). *Cyberattack disrupts European airports including Heathrow, Brussels*. Reuters.

Reuters. (2025b, December 12). *Berlin summons Russian ambassador over increase in hybrid attacks*. Reuters.

Romadhon, F. W., & Salman, M. (2025). Development of cyber attack scenarios for training local government cyber incident response teams using the MITRE ATT&CK framework

and Cyber Kill Chain. *Jurnal Pendidikan dan Teknologi Indonesia, 5*(5), 1265–1279. https://doi.org/10.52436/1.jpti.715

Sarjito, A. (2024). Formation of the TNI cyber force: A strategic and policy analysis. *Defense and Security Studies, 5*, 74–83. https://doi.org/10.37868/dss.v5.id272

Shin, Y., Kwon, H., Jeong, J., & Shin, D. (2024). A study on designing cyber training and cyber range to effectively respond to cyber threats. *Electronics, 13*(19), Article 3867. https://doi.org/10.3390/electronics13193867

Sutomo, A., Thamrin, S., Widodo, P., & Reksoprodjo, Y. (2025). Membangun ketahanan digital: Pengembangan model strategi pertahanan siber berbasis manajemen risiko. *Temali: Jurnal Pembangunan Sosial, 8*(1), 29–40. https://doi.org/10.15575/jt.v8i1.38690

Toth, R., Dubniczky, R. A., Limonova, O., & Tihanyi, N. (2025). *Sustaining cyber awareness: The long-term impact of continuous phishing training and emotional triggers* (arXiv:2510.27298). arXiv. https://doi.org/10.48550/arXiv.2510.27298

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. (2022). Ancaman serangan siber pada keamanan nasional Indonesia. *Jurnal Kewarganegaraan, 6*(1), 2319–2327.

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

Wenger, E. (1998). *Communities of practice: Learning, meaning, and identity*. Cambridge University Press.