Journal of World Science
Vol. 5, No. 11, November 2026, pp 935-956
E-ISSN: 2828-9307
https://doi.org/10.58344/jws.v5i11.1720

DEVELOPMENT OF CYBER AND SPACE CURRICULUM AT INDONESIAN AIR FORCE ACADEMY FOR DIGITAL TRANSFORMATION

Sya'ban Tri Hernawan*, Usni Hasanudin
Universitas Muhammadiyah Jakarta, Indonesia
Email : syabantri@gmail.com*, usnihasanudin@gmail.com

Keywords:
space and cyber curriculum; curriculum policy; digital transformation of tni au; cyber security; space.

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

Copyright © 2026 by Sya'ban Tri Hernawan, Usni Hasanudin. Published by Riviera Publishing

ABSTRACT

The digital transformation of the Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) requires personnel with advanced competencies in operating and securing cyber systems and utilizing space-based technologies. Although the Indonesian Air Force Academy (Akademi Angkatan Udara, AAU) has established a Space and Cyber Study Program, its curriculum continues to face gaps between academic content and operational requirements, alongside limitations in curriculum governance and policymaking processes. This study aimed to examine the curriculum's substantive content and policy development processes, assess its alignment with the Indonesian National Qualifications Framework (Kerangka Kualifikasi Nasional Indonesia, KKNI) and the Air Force's digital transformation objectives, evaluate implementation effectiveness, and formulate curriculum development and governance strategies. A qualitative case study approach was employed, incorporating interviews, observations, and document analysis. The findings revealed partial curriculum alignment, as program learning outcomes (Capaian Pembelajaran Lulusan, CPL) had not been systematically mapped to the European Digital Competence Framework (DigComp), and no operational competency matrix explicitly linked learning outcomes to Agile Combat Employment (ACE) and Joint All-Domain Operations (JADO) requirements. Curriculum implementation was constrained by limited cyber range capacity, examination-oriented assessment practices, and the absence of integrated industry-recognized certification pathways. Furthermore, curriculum policymaking followed a predominantly top-down approach, with approval processes taking approximately 6–12 months, limited stakeholder participation, and no standardized procedures or accelerated revision mechanisms. Based on these findings, the study proposed a curriculum development blueprint encompassing the revision and realignment of program learning outcomes, competency-to-mission mapping, expanded practical training, integration of professional certifications, participatory standard operating procedures, establishment of a representative curriculum board, digitalization of administrative processes, and systematic utilization of graduate tracer studies and learning analytics.

INTRODUCTION

The modernization of air operations over the past decade has been characterized by the growing importance of cyber and space operations and increasingly sophisticated threats targeting command-and-control (C2) networks, strategic sensors, and satellite infrastructure . Electronic warfare activities, including jamming and spoofing, as well as cyber intrusions into mission-critical networks, can degrade situational awareness, positioning, navigation, and timing (PNT) accuracy, and the effectiveness of targeting processes. Many air forces have increasingly recognized cyberspace and space as distinct operational domains rather than merely supporting functions, creating new requirements for military education curricula. These requirements include mission-oriented cybersecurity competencies, an understanding of satellite communications architectures, and the ability to integrate cybersecurity measures and system hardening into operational tactics, techniques, and procedures (TTPs). At the regional level, Southeast Asian countries have become increasingly dependent on commercial and government satellite services for communications, remote sensing, and navigation. This dependence has expanded the potential attack surface of interconnected and cross-border critical infrastructure, necessitating interoperability in operational procedures, data standards, access control, and incident response across multiple domains. Consequently, cyber and space curricula in regional defense education institutions must integrate technical competencies, risk governance, and principles of regional cooperation to address emerging security challenges (ASEAN, 2021).

At the national level, Indonesia's defense digital transformation agenda requires the Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) to strengthen data-driven operational capabilities, improve maintenance reliability through electronic logbooks and condition-based maintenance (CBM), and enhance the security and resilience of command-and-control architectures. Contemporary operational concepts, particularly Agile Combat Employment (ACE), emphasize the ability to maneuver, disperse forces, sustain operations, and maintain connectivity in contested environments. These requirements demand personnel capable of managing cybersecurity risks while effectively employing space-based capabilities, including intelligence, surveillance, and reconnaissance (ISR), PNT services, and satellite communications (SATCOM), as operational force multipliers. Accordingly, military graduate competency profiles must extend beyond traditional aeronautical knowledge and airmanship to encompass mission network security, SATCOM planning, and data analytics for tactical decision-making. These competencies are consistent with broader national priorities for strengthening the quality and operational relevance of military education (Markas Besar TNI, 2019).

At the institutional level, preliminary assessments indicated that the Indonesian Air Force Academy (Akademi Angkatan Udara, AAU) had not fully integrated cyber and space learning modules, cross-domain simulations, work-integrated learning, and industry-recognized certification pathways into its curriculum. Practical training infrastructure, including cyber ranges and SATCOM or microsatellite simulation facilities, also remained limited. These curricular and infrastructural constraints were compounded by the absence of standardized procedures for proposing, reviewing, approving, and implementing curriculum revisions. Furthermore, stakeholder participation involving operational units, instructors, cadets, and industry partners had not been systematically institutionalized or documented. Curriculum

revision processes remained predominantly top-down, potentially limiting their responsiveness to evolving operational requirements and technological developments. Therefore, this study examined both curriculum content and the associated policy development processes to formulate an integrated and sustainable curriculum improvement strategy aligned with the Indonesian Air Force's digital transformation objectives.

Previous research relevant to this study has examined digital transformation in military education, e-learning quality, information and communication technology (ICT) management at AAU, educational innovation, organizational factors, and military curriculum development. However, these research areas have generally been addressed separately, leaving limited understanding of how cyber and space competencies, operational mission requirements, and curriculum governance processes can be systematically integrated within a military academy. Table 1 summarizes the relevant studies, identifies their research gaps, and highlights their contributions to the conceptual and institutional foundations of the present investigation.

Table 1. Matrix of previous studies

Author/Year	Focus/Findings	Weakness/Gap	Relevance to this research
Lufti (2022)	Quality of e-learning-based education services at the Indonesian Military Academy	Does not address space–cyber competencies, LVC/cyber range, or certification	Reinforces the need for lecturer and facility readiness when the Space–Cyber curriculum is implemented
Fadillah & Yuniko (2023)	ICT management development at AAU; ICT 5.0 (AI, IoT, big data)	Conceptual with limited empirical evidence; does not cover satcom/microsatellite simulation or mission network security	Informs the need for a lab/simulation map and data-analytics integration
Bentri & Hidayati (2022)	Development of a digital pedagogical curriculum	Generic; not specific to military, cyber, or space education	Supports the design of innovative teaching methods (project-based learning, simulation)
Airyq et al. (2023)	Effect of competence, leadership, and organizational culture on performance	Not in the domain of military curriculum; does not map digital competencies or certification	Highlights the importance of leadership buy-in and a quality culture
Setiawan et al. (2025)	Digital competency-based military curriculum to support joint operations interoperability	Does not discuss the curriculum policy process	Basis for digital curriculum substance, complemented by policy analysis at AAU
Jevtić et al. (2024)	Optimization and review of military academy curricula	Focuses on curriculum content, not policy mechanisms	Supports the importance of an adaptive curriculum policy
Publico et al. (2026)	Integration of national security interests into military academy curricula in four countries	Does not discuss the governance of curriculum change	Reference for curriculum policy based on national security interests
Wahrobun et al. (2019)	Curriculum development policy for cadets of the Indonesian Naval Academy	Focuses on the curriculum product, not the policy process	Example of curriculum development within TNI

Source: Compiled from previous studies

These studies indicate that research on military education curricula, both in Indonesia and internationally, has predominantly focused on curriculum content and structure. From a political science and public policy perspective, however, an important dimension remains insufficiently examined: how curriculum policies are formulated, approved, implemented, and revised within hierarchical military institutions. Publico et al. (2026) provide a macro-level perspective on curriculum policy content but do not extensively examine the actors involved, the participation of instructors and operational units, or the time required to approve curriculum revisions. Similarly, Jevtić et al. (2024) emphasize the importance of continuous curriculum review but offer a predominantly normative rather than process-oriented analysis. Methodologically, limited research has integrated curriculum content evaluation, using approaches such as the Context, Input, Process, and Product (CIPP) model or gap analysis, with policy process mapping and stakeholder analysis. This integration is particularly relevant to military education, where established chains of command and bureaucratic procedures influence curriculum development and institutional decision-making.

The novelty of this study lies in integrating curriculum development with public policy analysis, two perspectives that have generally been examined separately in military education research. Methodologically, the study applied the policy cycle framework developed by Howlett et al. (2020) to examine curriculum revision processes within Indonesian military education, integrating it with the CIPP evaluation model and stakeholder analysis. This combined approach provided a framework for examining both curriculum content and the institutional mechanisms governing its development and revision. Substantively, the study sought to formulate a curriculum development blueprint alongside governance recommendations, including participatory standard operating procedures (SOPs) for curriculum revision, bottom-up proposal mechanisms involving operational units, and the establishment of a representative curriculum board. Contextually, the relatively recent establishment of the Space and Cyber Study Program at the Indonesian Air Force Academy (Akademi Angkatan Udara, AAU) provided an opportunity to examine curriculum development within an emerging military education discipline. The findings were expected to offer transferable insights for curriculum governance and development across other educational institutions within the Indonesian National Armed Forces (Tentara Nasional Indonesia, TNI), subject to institutional differences and operational requirements.

The theoretical framework integrated five complementary perspectives. First, curriculum development theory conceptualized curriculum development as a continuous process involving needs assessment, planning, implementation, and evaluation. Within military education, curriculum objectives are informed by strategic defense requirements and operational competency profiles. These objectives are subsequently translated into program learning outcomes (Capaian Pembelajaran Lulusan, CPL), instructional content, semester learning plans (Rencana Pembelajaran Semester, RPS), and performance-based competency assessments (Bachri, 2018; Ornstein & Hunkins, 2018). Second, the European Digital Competence Framework for Citizens (DigComp) provided a reference for examining digital competencies across five domains: information and data literacy, communication and collaboration, digital content creation, safety, and problem-solving. These domains informed the assessment of competency integration and the potential application of project-based and practice-oriented

learning approaches (Ferrari, 2013; Redecker & Punie, 2017). Third, the CIPP evaluation model provided a systematic framework for assessing curriculum context, inputs, processes, and products, facilitating evidence-based evaluation of curriculum relevance, resource adequacy, implementation quality, and educational outcomes (Stufflebeam & Zhang, 2017; Stufflebeam, 2003).

Fourth, the study employed the policy cycle framework developed by Howlett et al. (2020) to analyze curriculum governance through five interconnected stages: agenda setting, policy formulation, decision-making, implementation, and evaluation. Within the AAU Space and Cyber curriculum, these stages involved stakeholders with varying levels of authority, responsibility, and institutional interests, including academy leadership, curriculum committees, instructors, operational units, and industry or professional certification partners. Stakeholder analysis complemented this framework by identifying the relative influence, interests, and participation mechanisms of relevant actors within curriculum decision-making processes (Buse et al., 2012). Fifth, incrementalism provided a theoretical perspective for understanding gradual curriculum changes within hierarchical and bureaucratic institutions. According to Lindblom (1959), policymakers frequently operate under constraints involving information, time, cognitive capacity, and institutional resources, leading them to favor successive limited comparisons and incremental adjustments over comprehensive policy reforms. Within military education, this perspective helped explain why curriculum revisions may involve adjustments to credit allocations, the introduction of elective courses, or modifications to semester learning plans rather than extensive structural reforms. Accordingly, feasible improvement strategies should consider institutional constraints while establishing mechanisms for more timely and responsive incremental curriculum adjustments.

The integration of these theoretical perspectives produced three central propositions. First, curriculum quality was conceptualized as dependent not only on the relevance and coherence of its substantive content but also on the effectiveness of the policy processes governing its development and implementation. Second, curriculum reform within hierarchical military institutions was expected to follow predominantly incremental patterns, requiring improvement strategies that accommodated bureaucratic procedures, institutional authority, and established chains of command. Third, meaningful stakeholder participation, particularly involving instructors, laboratory personnel, cadets, and operational units, was considered essential for maintaining curriculum responsiveness to evolving operational requirements. Together, these propositions established an integrated analytical framework linking curriculum substance, policy governance, and stakeholder participation. The conceptual relationships among the research questions, theoretical perspectives, and expected analytical outputs are presented in Figure 1.

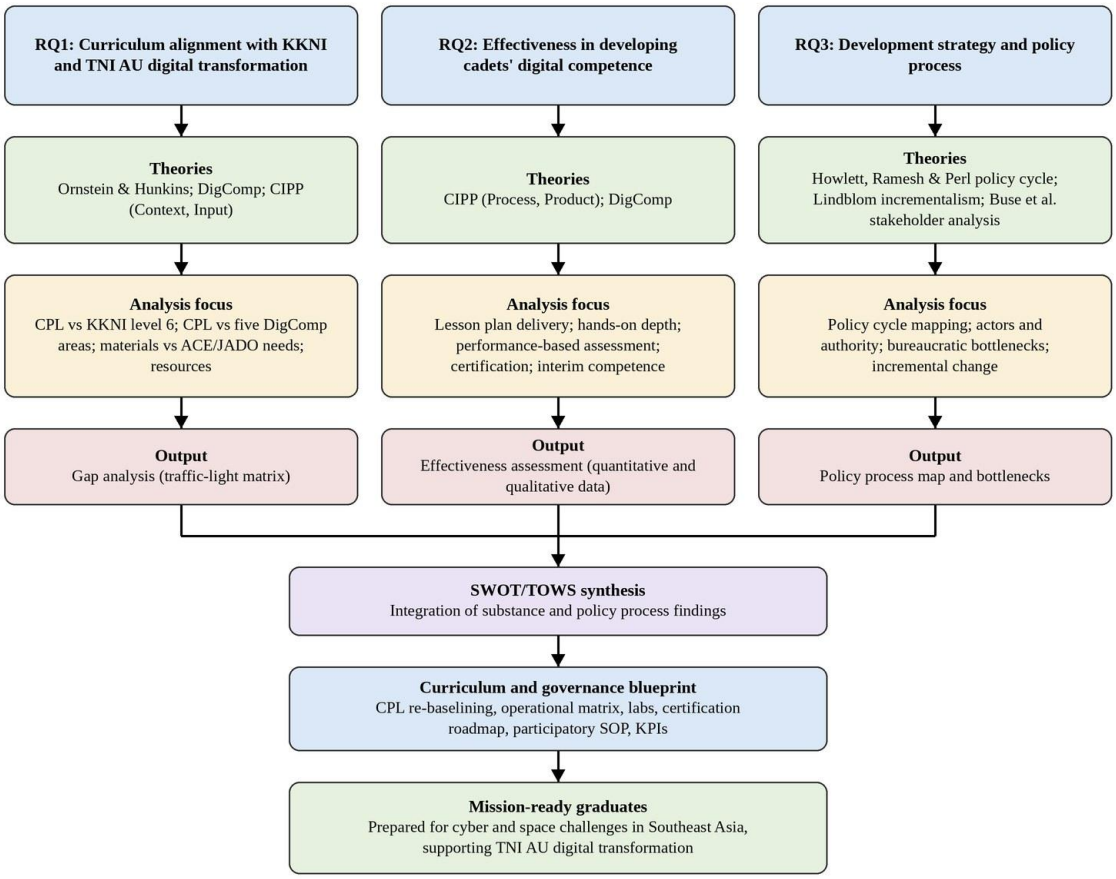

Figure 1. Conceptual framework

Source: Developed by the authors, 2026

Based on this background, the study addressed the central research question of how the development of the Space and Cyber Study Program curriculum could enhance cadets' digital competencies in support of the Indonesian Air Force's (Tentara Nasional Indonesia Angkatan Udara, TNI AU) digital transformation. Specifically, the study aimed to (1) assess the alignment of the Space and Cyber curriculum with the Indonesian National Qualifications Framework (Kerangka Kualifikasi Nasional Indonesia, KKNI), outcome-based education (OBE) principles, and the digital transformation requirements of TNI AU; (2) evaluate the effectiveness of curriculum implementation in developing cadets' digital competencies to address emerging cyber and space security challenges; and (3) analyze curriculum governance and formulate development and implementation strategies aligned with TNI AU operational requirements and the evolving cyber and space security environment in Southeast Asia, with particular emphasis on policy formulation, curriculum revision mechanisms, institutional governance, and stakeholder participation.

METHOD

This study employed a qualitative case study approach incorporating a systems perspective to examine the Space and Cyber Study Program at the Indonesian Air Force Academy (Akademi Angkatan Udara, AAU). The investigation focused on understanding the context, implementation processes, and outcomes of curriculum development, encompassing the formulation of program learning outcomes (Capaian Pembelajaran Lulusan, CPL), syllabus

design, laboratory and simulation-based training, and monitoring and evaluation mechanisms. These components were examined in relation to the operational requirements of the Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) and evolving regional cyber and space security challenges. The case study approach facilitated an in-depth examination of curriculum development and implementation within its institutional context using multiple sources of evidence (Yin, 2018). The Context, Input, Process, and Product (CIPP) evaluation framework was integrated to support systematic assessment and the formulation of evidence-based curriculum improvement recommendations (Creswell & Poth, 2018). The research was conducted at AAU, focusing on the curriculum management unit, the Space and Cyber Study Program, and supporting educational facilities, including laboratories, simulators, and the learning management system (LMS). Data collection complied with military institutional protocols, including authorization procedures, access restrictions, information classification requirements, and confidentiality agreements. The study was conducted from September 2025 to May 2026 and comprised four stages: preparation, data collection, data analysis, and report preparation and finalization.

Informants were selected through purposive sampling based on their involvement in curriculum development and implementation, expertise in cybersecurity and space technologies, understanding of operational requirements, and experience with professional certification partnerships or information security governance. This sampling strategy prioritized participants capable of providing relevant, in-depth information about curriculum content, implementation practices, and institutional decision-making processes (Patton, 2015). The number and composition of informants were determined iteratively, with recruitment continuing until sufficient information had been obtained and data saturation was achieved. The categories and characteristics of the informants are presented in Table 2.

Table 2. List of informants

No	Informant	Number/Code	Information explored
1	AAU Directorate of Studies – Kasibangorgjemen	1 person/IP1	Curriculum policy and approval process
2	Head of Space Sub-Department, Space and Cyber Program	1 person/IP2	CPL formulation, course structure, and curriculum evaluation
3	Lecturers/Instructors	2 persons/IP3, IP4	Curriculum implementation and learning development needs
4	Laboratory Staff, Space and Cyber Program	1 person/IP5	Support of facilities for practical learning
5	Cadets of the Space and Cyber Program	3 persons/IP6, IP7, IP8	Perceptions and experiences of curriculum implementation

Source: Research data, 2026

Data were collected through semi-structured interviews, nonparticipant observations of classroom instruction, laboratory activities, and simulation exercises, and document analysis. The interviews explored curriculum policymaking, decision-making processes, and implementation experiences, focusing on competency requirements, program learning outcomes (Capaian Pembelajaran Lulusan, CPL), instructional materials and methods, performance-based assessments, professional certification integration, and educational infrastructure. Observations were conducted using a structured checklist to evaluate the implementation of semester learning plans (Rencana Pembelajaran Semester, RPS), the extent

of practical training, the integration of standard operating procedures (SOPs) and tactics, techniques, and procedures (TTPs), information security practices, and the alignment of practical activities with program learning outcomes. The documents examined included CPL and Indonesian National Qualifications Framework (Kerangka Kualifikasi Nasional Indonesia, KKNI) documentation, curriculum and course mapping documents, RPS, laboratory and simulation SOPs, laboratory development plans, certification guidelines, curriculum governance policies, assessment results and rubrics, and Indonesian Air Force policies concerning digital competencies. Classified documents were excluded from data collection, and research records were managed in accordance with institutional information security and need-to-know requirements.

Data analysis was conducted in four stages. First, qualitative data were analyzed using the Miles–Huberman framework, comprising data condensation, data display, and conclusion drawing and verification, supported by thematic coding to identify recurring patterns and institutional issues (Miles et al., 2014). Second, a gap analysis was performed by mapping each CPL against DigComp competency indicators, KKNI requirements, and operational competency demands associated with Agile Combat Employment (ACE) and Joint All-Domain Operations (JADO). The results were organized into a three-category alignment matrix: green (fully aligned), yellow (partially aligned), and red (not aligned). Identified gaps represented discrepancies between expected competencies and documented curriculum provisions or learning outcomes (Clark & Estes, 2008). Third, these gaps were evaluated across the four dimensions of the Context, Input, Process, and Product (CIPP) model to identify areas requiring curriculum improvement and prioritize interventions (Stufflebeam, 2003). Fourth, the findings were synthesized using strengths, weaknesses, opportunities, and threats (SWOT) analysis and a threats, opportunities, weaknesses, and strengths (TOWS) matrix. The TOWS analysis generated four strategic combinations—strengths–opportunities (SO), weaknesses–opportunities (WO), strengths–threats (ST), and weaknesses–threats (WT)—to formulate curriculum development strategies based on internal institutional conditions and external operational requirements (Weihrich, 1982). The resulting recommendations were consolidated into a curriculum development blueprint accompanied by measurable and auditable performance indicators.

The trustworthiness of the findings was strengthened through triangulation across data sources, collection methods, and observation periods (Patton, 1999), member checking with key informants (Lincoln & Guba, 1985), peer debriefing, and maintenance of an audit trail and chain of evidence (Yin, 2018). Credibility and dependability were supported by systematic documentation of research procedures, data collection protocols, analytical decisions, and coding frameworks (Shenton, 2004). Confirmability was addressed through reflexive memoing to document researcher assumptions and interpretations, while transferability was supported by detailed descriptions of the institutional, operational, and educational context of the Indonesian Air Force Academy.

RESULTS AND DISCUSSION

Overview of AAU and the Space and Cyber Program

AAU is a military higher education institution under TNI AU located in Sleman Regency, Special Region of Yogyakarta, led by a Governor, with the main task of producing professional

TNI AU officers with the rank of Second Lieutenant. AAU has opened the D-IV Cyber and Space Defense Engineering Study Program (known as the Space and Cyber program) in line with the direction of the Chief of Staff of the Air Force to prepare human resources skilled in cyber and space. The program is managed through a dual-track structure consisting of the Head of Department/Head of Study Program, the Heads of the Cyber and Space Sub-Departments, and the Heads of the Cyber and Space Sections. Its CPL refer to the KKNI framework and the National Higher Education Standards (Kementerian Pendidikan dan Kebudayaan, 2020), with an emphasis on forming officers who master cyber defense and space technology, can analyze and respond to cyber threats and space dynamics, make tactical decisions based on cyber and space intelligence data, and uphold professional ethics and the chain of command.

The program is supported by a rocket and space laboratory, a satellite laboratory and simulator with a channel emulator, a rocket simulator using MATLAB and Simulink, cyber training through virtual laboratories such as TryHackMe with partner institutions including BSSN and the State Cyber and Cryptography Polytechnic, and a learning management system (LMS). The quantity and capacity of some facilities, particularly the cyber range and satellite simulator, still need to be improved to accommodate all learning outcome targets and the standards for space education facilities. The baseline condition of the facilities is summarized in Table 3.

Table 3. Baseline condition of laboratories and simulation facilities

Facility	Current condition
Cyber range	1 unit, capacity of 10 users, not yet integrated with LVC
Satellite simulator	2 units, only for basic demonstration
Rocket simulator	1 unit (based on MATLAB/Simulink)
Supporting laboratories	Electronics, digital systems, electrical circuits (fairly good condition)
Learning management system	Used as a material repository, assignment, and communication tool; learning analytics not yet developed

Source: Research findings, 2026

Curriculum Substance

Context: Alignment of CPL with KKNI and DigComp

The current CPL refer to KKNI level 6 for the Diploma IV level, based on the curriculum document of the TNI AU Defense Study Program (Amendment II of 2025) (Kurikulum Pendidikan Prodi Pertahanan TNI AU, n.d.). However, several significant gaps remain. First, a matrix linking CPL with DigComp has not been explicitly developed. The curriculum refers more to NIST SP 800-181 (NICE Framework) for cyber competencies (National Institute of Standards and Technology, 2020); data literacy and problem solving are relatively accommodated, safety is fairly strong through courses such as Network Security, Cryptography, Security Operations Center, Penetration Tester, and Digital Forensics, whereas communication and collaboration and digital content creation are less explicit. As the Head of the Space Sub-Department stated: “The program does not yet have a matrix that explicitly links CPL with DigComp. What we use is the NICE Framework for the cyber domain. For the space domain, no digital competence standard has been formally adopted. We recognize this as a shortcoming” (IP-02).

Second, several mission-level technical competencies are not yet reflected in the CPL, such as satcom planning, mission network defense, and incident response in constrained

operational environments (forward airfields under the ACE concept). Third, the gap analysis of curriculum documents produced a traffic-light matrix in which network security, cryptography, basic programming, digital systems, and digital signal processing are aligned (green); orbital mechanics, spacecraft propulsion, security incident response, and digital forensics are partial (yellow); and satcom planning for joint missions, tactical mission network defense, and real-time space intelligence data analytics are empty (red). These gaps are mainly caused by CPL that remain too general and have not been operationally derived into course sub-CPL, as CPL formulation has been driven more by the availability of lecturers and facilities than by systematic job task analysis. Table 4 summarizes the status of CPL against DigComp and KKNI.

Table 4. Status matrix of CPL, DigComp, and KKNI

DigComp area	Related CPL/courses	KKNI level	Traffic-light status	Notes
Data literacy	Statistics and Probability, Digital Signal Processing	6	Green	Competence well accommodated in the curriculum
Communication and collaboration	English, Leadership	5–6	Yellow	Competence exists but is not explicitly stated in technical CPL
Digital content creation	Programming, Databases	6	Green	Supported by fairly adequate practicum learning
Safety	Network Security, Cryptography, SOC, Penetration Tester, Forensics	6–7	Green (theory), Yellow (mission practice)	Good theoretical mastery, but operational practice is limited by facilities
Problem solving	Final Project, Final Project Proposal, Capita Selecta	6	Yellow	Still dominated by simulation; few real operational scenarios

Source: Research findings, 2026

The analysis of RPS and syllabi further revealed four findings regarding the gap between materials and the demands of ACE and Joint All-Domain Operations (JADO). First, Satellite Communication Systems (SA-1358) and its practicum (SA-1359) remain oriented toward link budget, propagation, and modulation calculations, with little room for jamming and anti-jamming scenarios, because the satellite simulator can only simulate ideal conditions: “For satcom planning under jamming, for example, it is still limited to theory. Practice cannot yet be done because the satellite simulator can only simulate ideal conditions” (IP-02). Second, Penetration Tester (SA-1349) and Security Incident Response (SA-1362) are theoretically adequate, but practice is very limited because the cyber range accommodates only 10 users. Third, Orbital Mechanics (SA-1337) and Spacecraft Propulsion (SA-1324) are considered highly theoretical; practicums use MATLAB and STK but are never tested with real data from operational satellites, and reading two-line elements (TLE) and predicting satellite passes are not explicitly included in the RPS. Fourth, no course specifically addresses mission network defense in forward operating bases with limited connectivity, as Network Security (SA-1314) still focuses on conventional office network security. These gaps stem from limited simulation facilities that can replicate operational conditions, the lack of input from operational units in syllabus development, and overly general CPL.

Input: Course Structure, RPS, and Assessment

The program comprises 145–147 credits depending on electives. Semesters 1–4 contain basic military, engineering, and introductory cyber and space courses; semesters 5–6 cover core courses such as Penetration Tester, Security Operations Center, Satellite Communication Systems, Orbital Mechanics, and Cryptography; and semesters 7–8 focus on electives and the final project. Although this flow is logical, there is redundancy—for example, Operating Systems (semester 2) and Basic Computer and Programming (semester 3) overlap on computer architecture—and emptiness in critical topics such as mission network defense and satcom planning. Most RPS contain learning outcomes, study materials, learning strategies, and assessment, but their quality varies: hands-on targets in practicum courses are often not achieved due to equipment limitations, while theoretical courses rely on lectures and calculation assignments. Assessment is still dominated by written exams; capture-the-flag assessment has been attempted in Penetration Tester but can only be conducted when the cyber range is available. From the CIPP-Input perspective, the curriculum design is structurally adequate, but there is a gap between RPS documents and implementation capacity and a lack of a matrix linking CPL with appropriate assessment methods.

Process: Effectiveness of Lectures, Practicums, and Simulations

Observation of core courses in semesters 5 and 6 showed that RPS delivery varies. Courses with hardware-dependent practicums do not reach the targeted practice hours, whereas software-based practicums such as MATLAB for Digital Signal Processing can be carried out as planned. A lecturer explained: "The cyber range can only accommodate 10 users, while there are 30 cadets per cohort. The target of 4 practice sessions per semester has never been achieved; realistically 2. The satellite simulator is also limited, so vehicle launch system practice can only be done 1–2 times per semester" (IP-04). Cadets considered capture-the-flag in Penetration Tester their most memorable practical experience, but it took place only once or twice a semester, and most practicums were structured, module-based activities rather than open-ended scenarios. Changing assessment practices was also slow: "I once proposed that the Penetration Tester assessment use capture-the-flag instead of a written exam. The program responded positively, but implementation took one semester because the RPS had to be revised and approved by the Head of Department" (IP-03).

AAU does not yet have a cyber range integrated with live-virtual-constructive (LVC) simulation, so cyber training remains separate from flight or satellite simulation, even though under ACE and JADO cyberattacks and space disruptions occur simultaneously with air operations. Cadets felt confident using basic tools such as Wireshark, Nmap, and Metasploit but not yet ready for complex scenarios such as incident response on an operating network: "The material is quite relevant, but we feel underprepared for real scenarios. We know the concepts of firewalls, IDS, and how satellites work, but we have never tried to configure devices in a real attack scenario" (IP-06). From the CIPP-Process perspective, implementation effectiveness is not yet optimal due to limited capacity and integration of simulation facilities, failure to achieve RPS practice targets, and insufficient training in open and integrated scenarios.

Certification Pathways and Industry Partnerships

AAU has established relationships with BSSN, the State Cyber and Cryptography Polytechnic, and EC-Council for CEH certification (EC-Council, 2023), but these memoranda

of understanding have not been followed by mandatory integration of certification into the curriculum; certification remains incidental, taken only by interested cadets or lecturers assigned to training. Guest lectures by BSSN practitioners have occurred, but there is no continuous co-teaching scheme, and classification and NDA constraints often hinder the sharing of operational material. As a result, cooperation is often limited to MoUs without meaningful technical implementation, and user units expect the future curriculum to integrate at least one mandatory certification. From the CIPP-Input and Process perspectives, the certification and industry partnership aspect is still very weak.

Product: Interim Competence Achievement

Because the program has run for only two years and has no graduates, the Product evaluation focuses on interim competence achievement and projected readiness. Cadets in semesters 3 and 4 obtained average grades of B+ to A− in courses such as Digital Systems (SA-1309), Basic Computer and Programming (SA-1307), and Introduction to Cyber (SA-1304), but these results must be interpreted carefully because early-semester assessment is dominated by written exams and structured assignments (Laporan Evaluasi Pelaksanaan Pendidikan AAU, 2025). Network Security is introduced in semester 3 with only one practicum credit, so cadets' understanding remains introductory. Feedback from on-the-job training supervisors indicates that cadets can explain satellite communication theory well but remain awkward when operating unfamiliar hardware. Thus, the first graduates are projected to have solid theoretical knowledge but still require improvement in mission-level practical skills; this evaluation remains tentative until tracer study data become available.

Curriculum Policy Process

The curriculum policy process was mapped using the policy cycle model (Howlett et al., 2020), stakeholder analysis (Buse et al., 2012), and CIPP, based on interviews and policy documents, including the Decree of the Chief of Staff of the Air Force No. Kep/467/XII/2021 on the Technical Guidelines for Curriculum Development (Keputusan Kepala Staf Angkatan Udara Nomor Kep/467/XII/2021, 2021). The findings for each stage are summarized in Table

Table 5. Mapping of the curriculum policy cycle

Policy stage	Main findings
Agenda setting	Sources: internal annual evaluation, directives from TNI AU leadership (e.g., Amendment II of 2025 driven by the TNI Commander's Telegram No. ST/239/2025 on reduced education time), regional threat developments, and input from operational units; cadets and industry partners are almost never sources of the agenda; agenda setting is top-down and reactive
Formulation	Carried out by an ad hoc curriculum team (Head of Program, Heads of Sub-Departments and Sections, lecturers, Directorate of Studies); lecturer participation is often ceremonial; revisions expected to take 2–3 months are often delayed
Adoption	Layered chain of command: Head of Department → Directorate of Studies → AAU Curriculum Board → Governor → Chief of Staff of the Air Force; minor revisions take 1–2 months and major revisions 6–12 months; no fast-track mechanism
Implementation	Suboptimal socialization of new policies; gap between policy design and field capacity; weak cross-department coordination; no systematic monitoring instrument

Policy stage	Main findings
Evaluation	End-of-semester evaluation meetings are anecdotal without key performance indicators; tracer studies cannot yet be conducted; no fast feedback loop from the field to policymakers

Source: Research findings, 2026

At the agenda-setting stage, revision issues arise from internal evaluation, leadership directives, threat developments, and operational unit input. Amendment II of 2025 was partly driven by an instruction to adjust to reduced education time (Surat Telegram Panglima TNI Nomor ST/239/2025, 2025), while threat information is not systematically translated into curriculum proposals because no procedure links intelligence units with the curriculum team. At the formulation stage, a lecturer described: "We are invited to meetings and given the opportunity to provide input, but the final draft that circulates is already different from what we proposed," indicating a concentration of authority. At the adoption stage, the Kasibangorgjemen confirmed: "The curriculum revision process must pass through several echelons, from the program, the Head of Department, the Directorate of Studies, the Curriculum Board, the Governor, up to the Chief of Staff. For minor revisions it can take 3–4 months, but for changes in course structure it can take 10–12 months. There is no special pathway for urgent topics" (IP-01). Amendment II, ratified in December 2025, had been in formulation since early 2025, a total of about 12 months.

At the implementation stage, some lecturers learned of changes in course structure or RPS only when the new semester was about to begin. Laboratory staff were not involved in policy planning, so unrealistic implementation burdens were felt only after the policy took effect; for example, the additional Penetration Tester practice hours in Amendment II were not accompanied by increased cyber range capacity or additional technicians. Monitoring by the Directorate of Studies relies on periodic reports without checklists or measurable indicators, so implementation gaps remain undetected until the end of the period. At the evaluation stage, end-of-semester meetings tend to be anecdotal, tracer studies cannot yet be conducted, and input from operational units hosting cadets for on-the-job training is not structured or documented. Consequently, curriculum policy lags behind fast-moving cyber and space threats.

The stakeholder mapping in Table 6 shows an imbalance between actors with power (leadership) and actors with implementation knowledge and interest (lecturers, laboratory staff, cadets), so curriculum policy tends to be top-down and less responsive to technical needs in the field.

Table 6. Mapping of actors by power and interest

Category	Actors	Role in the curriculum policy process
High power, high interest (dominant players)	Chief of Staff of the Air Force; AAU Governor; Head of the Cyber and Space Department	Final authority, ratification after the curriculum board, and initiation and approval of drafts at the department level
Medium power, high interest (players)	Directorate of Studies; Head of Program and Heads of Sub-Departments	Academic verifier without final veto; daily program management and initial drafting

Category	Actors	Role in the curriculum policy process
Low power, high interest (subjects)	Lecturers/instructors; laboratory staff; cadets; operational units	Implement or use the curriculum, but have no permanent representation or formal mechanism to provide input
Low power, low interest (crowd)	Industry partners/certification bodies; other curriculum board members	No significant role due to limited partnerships; formal power but low interest in the Space and Cyber field

Source: Research findings, 2026

Five main bottlenecks were identified: (1) a long approval flow in which every layer can return a draft for revision, which then repeats the entire flow; (2) the absence of a fast-track SOP for emergency revisions, so all changes must wait for the scheduled revision cycle, usually every two years: "There is no standard revision SOP. If I want to change the material, I do not know where to submit it. In the end I adjust it myself in class. This is not ideal because the change is not documented" (IP-04); (3) slow cross-unit coordination for courses involving other departments; (4) limited documentation and transparency, with no central database tracking the status of revision proposals, weakening institutional memory; and (5) procurement bureaucracy that is not synchronized with the curriculum cycle, as procurement of laboratory equipment can take 1–2 years. Applying CIPP to governance, the context is adequate but not optimal due to low responsiveness, the input is weak because no SOP for rapid revision or stakeholder participation exists and budgets and human resources are limited, the process is less effective because of bottlenecks and minimal participation, and the product is adequate but suffers from a relevance lag.

Integration of Substance and Policy Process Findings

The substance problems (CPL gaps, laboratory limitations, lack of certification) and the policy process problems (long revision flows, limited participation, weak documentation) are closely interrelated and form a feedback loop. First, a slow policy process prevents the curriculum from keeping pace with cyber and space threats that evolve in weeks, while the normal revision cycle takes 6–12 months. Second, a non-participatory process means that input from lecturers, laboratory staff, cadets, and operational units—those who best know facility constraints and real competency needs—is not accommodated, resulting in unrealistic policies. Third, an undocumented process causes a loss of institutional memory, so the same gaps may recur. Substance gaps are therefore symptoms rather than root causes of an unhealthy policy process.

The relationship is circular and mutually reinforcing. A slow and non-participatory process produces an outdated and unrealistic curriculum, which in turn creates demands for revision that cannot be accommodated; when ratified documents cannot be implemented, a credibility crisis encourages greater centralization in the next cycle, which further slows the process. This cycle has begun at the Space and Cyber program, as some lecturers bypass formal policy by informally adjusting materials in their own classes. This pattern is consistent with incrementalism (Lindblom, 1959): the layered adoption process and the absence of a fast-track mechanism encourage policymakers to choose changes that generate the least resistance rather than those that are substantively optimal. Viewed as an ecosystem of substance, actors, rules, and facilities, the curriculum shows serious imbalance: the rules are too rigid, actors with

implementation knowledge lack power, leadership is distant from technical constraints, and facilities do not grow as fast as substantive demands. Improvement thus cannot be limited to curriculum substance; the policy process must be fundamentally reformed.

SWOT Analysis and TOWS Strategy

The SWOT analysis was based on the field findings and stakeholder interviews and is presented in Table 7. Among the strengths, the existence of the program is evidence of leadership commitment, reflected in the Decree of the Chief of Staff of the Air Force No. Kep/13/I/2025 on the Curriculum of the TNI AU Defense Study Program and its amendments (Keputusan Kepala Staf Angkatan Udara Nomor Kep/13/I/2025, 2025). Opportunities arise from the urgent digital transformation agenda set out in strategic documents (Kementerian Pertahanan RI, 2021; TNI AU, 2021), defense innovation funding mechanisms, and regional cooperation (ASEAN, 2021). Threats include rapidly evolving cyber and space threats, including emerging technologies that reshape cybersecurity training, slow bureaucracy, and limited budgets that compete with other operational needs (Laporan Evaluasi Pelaksanaan Program Kerja dan Anggaran AAU, 2025).

Table 7. SWOT identification

Factor	Description
Strengths	Lecturers come from TNI AU operational units and understand field needs; leadership commitment through policy and the establishment of the Space and Cyber program; the first space and cyber program within TNI; core cyber and space courses are already available
Weaknesses	Digital competencies are not systematically mapped; cyber range and simulators are inadequate; the revision process is slow and less participatory; evaluation is still dominated by theory; no official competency certification pathway
Opportunities	Increasing need for space and cyber personnel; opportunities for benchmarking and knowledge exchange; CEH, CompTIA, and satellite certifications can be adopted; potential cooperation with BSSN, Kominfo, and industry; opportunity to become the space education center of TNI AU
Threats	The curriculum risks lagging behind threat dynamics; procurement and curriculum revision take a long time; facility development competes with operational needs; graduate competence risks not matching unit needs; many other institutions are developing the cyber field; education and defense policies change quickly

Source: Research findings, 2026

The TOWS matrix produced four complementary strategy groups, summarized in Table 8. The WT strategies (fast-track revision and periodic gap analysis) form the most urgent foundation because they concern the program's ability to withstand external threats; the WO strategies (CPL matrix and revision SOP) are the second priority because they address fundamental weaknesses; and the SO and ST strategies are medium- to long-term strategies that strengthen the program's position as a center of excellence.

Table 8. TOWS strategy formulation

Strategy	Main actions
SO (Strengths–Opportunities)	Accelerate the adoption of industry certification by leveraging certified lecturers and integrating certification material into RPS and final assessments; use first-mover status to build ASEAN regional networks through benchmarking and regional workshops

Strategy	Main actions
WO (Weaknesses–Opportunities)	Develop the CPL–DigComp–KKNI matrix with industry partners and certification bodies; propose a revision SOP as part of AAU's digital transformation roadmap with bottom-up proposals and revision cycles of 6 months (minor) and 2 years (major); build partnerships for a cyber range and satellite simulator through CSR schemes
ST (Strengths–Threats)	Establish the program as a center of excellence providing rapid recommendations to leadership on threat developments; build an early warning network with operational units through liaison officers and joint after action reviews
WT (Weaknesses–Threats)	Create a fast-track revision mechanism for critical topics approved temporarily by the AAU Governor; conduct a gap analysis every semester as the basis for revision proposals; prioritize a portable cloud-based or open-source cyber range; integrate the CPL–DigComp–KKNI matrix into accreditation documents

Source: Research findings, 2026

Recommendations for Curriculum Substance and Governance

Four substance recommendations were formulated. First, CPL should be re-baselined through job task analysis following NIST SP 800-181 (National Institute of Standards and Technology, 2020), actively involving operational units and industry partners to identify graduate roles (such as Cyber Defense Analyst, Satellite Communication Officer, and Space Situational Awareness Operator), key tasks, and the required knowledge, skills, and attitudes. Second, an operational matrix linking CPL, DigComp, KKNI, and ACE/JADO mission needs should serve as a living document that guides RPS, assessment, and evaluation. Third, practice hours in the cyber range and satcom simulator should be increased—in the short term through a virtual cloud-based cyber range with a target of at least four capture-the-flag sessions per semester and low-cost software-defined radio for satellite communication—and a data-analytics pipeline should be developed for data-based learning. Fourth, at least one industry certification (CompTIA Security+ or CEH for the cyber track, or satellite certification for the space track) should be integrated into compulsory courses in stages, with performance-based assessment instruments aligned with recognized standards (International Organization for Standardization [ISO], 2015).

Five governance recommendations were also formulated. First, a participatory curriculum revision SOP should regulate bottom-up proposals from lecturers, laboratory staff, cadets, and operational units, require a response within 14 working days, and establish a fast-track pathway with approval only up to the AAU Governor for temporary decisions. Second, a permanent and representative curriculum board should include the Head of Department, Head of Program, lecturer representatives, the Directorate of Studies, operational units, alumni, and industry partners, meeting at least every three months. Third, a periodic evaluation cycle every two years should use a measurable feedback loop with key performance indicators. Fourth, the administration of curriculum policy should be digitalized through a database of proposals, meeting minutes, document versions, and decisions. Fifth, tracer studies and LMS learning analytics should become the main triggers of curriculum revision, with learning analytics providing rapid feedback and tracer studies providing long-term feedback for structural revision.

Final Blueprint of the Space and Cyber Curriculum

The final blueprint is based on five principles: orientation toward operational needs, reference to national and international standards, participation and sustainability, integration of substance and policy process, and adaptability to changing threats. Structurally, the blueprint retains the current 145–147 credits but adds Mission Network Defense (2 credits) and Satellite Communication Planning for Military Operations (2 credits) in semester 5 or 6, merges redundant courses such as Basic Computer and Programming (SA-1307) and its practicum (SA-1308) into a single 3-credit course, and increases the practice weight of Penetration Tester (from 2 to 3 practice credits) and Satellite Communication Systems (from 1 to 2 practice credits). The core product is the operational matrix in Table 9.

Table 9. Operational matrix of CPL, DigComp, KKNI, and mission needs

CPL code	CPL formulation (summary)	DigComp area	KKNI level	Mission need (ACE/JADO)	Courses
CPL-1	Able to secure data communication networks in tactical environments	Safety	6	Protect the mission network from intrusion at forward operating bases	Network Security, Mission Network Defense
CPL-2	Able to plan satellite communication under jamming conditions	Problem solving	6	Respond to satellite communication disruption caused by electronic warfare	Satellite Communication Systems, Satcom Planning
CPL-3	Able to perform penetration testing and incident response	Safety	6	Identify and respond to cyberattacks on command-and-control systems	Penetration Tester, Security Incident Response
CPL-4	Able to analyze orbital data to support space situational awareness	Data literacy	6	Monitor enemy satellite movements and potential collisions	Orbital Mechanics, Satellite Technology
CPL-5	Able to work in multi-domain teams and communicate effectively	Communication and collaboration	5	Coordinate with land, sea, and air units in joint operations	Leadership, English, Bhuwana Paksa Exercise

Source: Research findings, 2026

The laboratory map sets short-term targets (one year) of a virtual cyber range accessible to 60 cadets simultaneously, two software-defined radio units, and two additional technicians, and medium-term targets (three years) of a permanent 30-user cyber range integrated with LVC, a satcom simulator with virtual reality, and a data-analytics pipeline using the ELK stack or Splunk. The certification roadmap consists of three stages: integration of certification material into RPS with pilot funding for the best 10–20% of cadets (years 1–2), one mandatory certification as a graduation requirement (years 2–3), and expansion to advanced certifications such as CEH, CISM, or OSCP and internships with industry partners (years 3–5). The performance indicators used to monitor the blueprint are summarized in Table 10.

Table 10. Performance indicators for monitoring the blueprint

Dimension	Indicator	Target
Curriculum substance	Achievement of practice targets in RPS	≥80%
	Certification exam results	Minimum passing rate of 70% for all cadets

Dimension	Indicator	Target
Policy process	Operational unit satisfaction with graduate readiness	Average score ≥4 out of 5
	Program response time to revision proposals	Average ≤14 working days
	Bottom-up proposals accommodated per year	≥50% of proposals received
	Time from initiation to ratification	≤3 months (minor); ≤6 months (major)
	Tracer study recommendations followed up in revisions	≥70%
Facilities and partnerships	Practice hours per cadet per semester	Increase of 50% from baseline within 2 years
	Active industry partners	At least 3 partners within 2 years

Source: Research findings, 2026

The blueprint is a dynamic document that will be updated according to threat dynamics, technological developments, and stakeholder input. Its success depends on the collective commitment of AAU and TNI AU: the AAU Governor is expected to ratify the participatory revision SOP and provide a budget for a virtual cyber range, the Chief of Staff of the Air Force is expected to support industry certification as part of the strategic digital transformation program, operational units are expected to provide input through the curriculum board and host cadets for more structured field practice, and the program is expected to prepare an annual action plan with clear milestones.

CONCLUSION

The Space and Cyber curriculum at the Indonesian Air Force Academy (Akademi Angkatan Udara, AAU) was designed with reference to Level 6 of the Indonesian National Qualifications Framework (Kerangka Kualifikasi Nasional Indonesia, KKNI) and included relevant core courses. However, its alignment with the digital transformation requirements of the Indonesian Air Force (Tentara Nasional Indonesia Angkatan Udara, TNI AU) remained partial. No operational competency matrix systematically linked program learning outcomes (Capaian Pembelajaran Lulusan, CPL) with the European Digital Competence Framework for Citizens (DigComp), KKNI requirements, and mission-specific competencies associated with Agile Combat Employment (ACE) and Joint All-Domain Operations (JADO). Critical operational competencies, including satellite communications (SATCOM) planning in contested electromagnetic environments, mission network defense, and real-time analysis of space-based intelligence, were not explicitly incorporated into the curriculum. Furthermore, CPL formulation was influenced primarily by instructor availability and existing educational facilities rather than systematic job-task analysis. Curriculum implementation also remained suboptimal, with learning achievements concentrated predominantly in the cognitive domain, while practical skills and professional attitudes received comparatively limited emphasis. These limitations were associated with insufficient cyber range and simulation capacity, examination-oriented assessment practices, and the absence of mandatory industry-recognized certification pathways. Curriculum governance was characterized by predominantly top-down decision-making, lengthy approval procedures lasting approximately 6–12 months, limited stakeholder participation, and inadequate documentation. The absence of accelerated revision

mechanisms, participatory standard operating procedures (SOPs), and measurable performance indicators further constrained the institution's ability to respond promptly to evolving cyber and space security requirements.

Based on these findings, the study recommended that AAU revise and realign its CPL through systematic job-task analysis, establish an operational competency matrix connecting learning outcomes with mission requirements, expand practical training through virtual cyber ranges and data analytics environments, and integrate at least one relevant industry-recognized professional certification into the curriculum. At the governance level, AAU should establish participatory curriculum revision SOPs incorporating bottom-up proposals from operational units and accelerated approval mechanisms for time-sensitive competency updates. A representative curriculum board should be established to conduct quarterly reviews, supported by a biennial comprehensive evaluation cycle with measurable performance indicators. Curriculum administration should also be digitalized, while graduate tracer studies and learning analytics should be systematically incorporated as evidence-based triggers for curriculum revision. Strengthening partnerships with operational units, industry stakeholders, and professional certification providers would further enhance the curriculum's relevance and practical applicability. Future research should examine the relationship between curriculum governance quality and graduate operational readiness through larger-scale tracer studies, conduct comparative assessments of cyber and space curricula across Southeast Asian military academies, evaluate the proposed curriculum blueprint following an implementation cycle, and develop validated performance-based assessment instruments and cost-effective, portable cyber range training environments.

FUNDING

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

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 thea uthors wherever possible. If you identify any issues, please contact us.

REFERENCES

Airyq, I. M., Hubeis, A. V. S., & Sukmawati, A. (2023). Pengaruh kompetensi, kepemimpinan dan budaya organisasi terhadap kinerja sumber daya manusia. *Jurnal Aplikasi Bisnis dan Manajemen, 9*(1), 285–295. https://doi.org/10.17358/jabm.9.1.285

ASEAN. (2021). *ASEAN cybersecurity cooperation strategy 2021–2025*. ASEAN Secretariat.

Bachri, B. S. (2018). *Curriculum development and implementation on higher education in Indonesia* [Conference paper]. Atlantis Press. https://doi.org/10.2991/ICEI-18.2018.106

Bentri, A., & Hidayati, A. (2022). The developing of digital pedagogical curriculum of primary education teachers in Indonesia. *Journal of Physics: Conference Series, 2309*, Article 012097. https://doi.org/10.1088/1742-6596/2309/1/012097

Buse, K., Mays, N., & Walt, G. (2012). *Making health policy* (2nd ed.). Open University Press.

Clark, R. E., & Estes, F. (2008). *Turning research into results: A guide to selecting the right performance solutions*. Information Age Publishing.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

EC-Council. (2023). *Certified Ethical Hacker (CEH) v12 technical content guide*. https://www.eccouncil.org

Fadillah, H., & Yuniko. (2023). Pengembangan manajemen information and communication technology di Akademi Angkatan Udara. *Jurnal TNI Angkatan Udara, 2*(2). https://doi.org/10.62828/jpb.v2i2.68

Ferrari, A. (2013). *DIGCOMP: A framework for developing and understanding digital competence in Europe*. Publications Office of the European Union. https://doi.org/10.2788/52966

Howlett, M., Ramesh, M., & Perl, A. (2020). *Studying public policy: Principles and processes* (4th ed.). Oxford University Press.

International Organization for Standardization. (2015). *Management system for private security operations — Requirements with guidance for use* [ISO Standard No. 18788:2015]. ISO.

Jevtić, D., Miljković, M., & Đorđević, M. (2024). Supplementing curriculum of the military academy for the purpose of providing education for country defence. *Vojno delo, 76*(4), 35–50. https://doi.org/10.5937/vojdelo2404035J

Kementerian Pendidikan dan Kebudayaan. (2020). *Peraturan Menteri Pendidikan dan Kebudayaan Nomor 3 Tahun 2020 tentang Standar Pendidikan Tinggi*. https://jdih.kemdikbud.go.id

Kementerian Pertahanan RI. (2021). *Peraturan Menteri Pertahanan Nomor 10 Tahun 2021 tentang Rencana Strategis Kementerian Pertahanan dan Tentara Nasional Indonesia Tahun 2020–2024*. Kementerian Pertahanan Republik Indonesia.

Keputusan Kepala Staf Angkatan Udara Nomor Kep/13/I/2025 tentang Kurikulum Pendidikan Program Studi Pertahanan TNI AU Akademi Angkatan Udara (2025).

Keputusan Kepala Staf Angkatan Udara Nomor Kep/467/XII/2021 tentang Petunjuk Teknis Pembinaan Kurikulum Pendidikan di Lingkungan TNI Angkatan Udara (2021).

Kurikulum Pendidikan Prodi Pertahanan TNI AU (Prodi Space and Cyber) (n.d.).

Laporan Evaluasi Pelaksanaan Pendidikan AAU Tahun 2025 (2025).

Laporan Evaluasi Pelaksanaan Program Kerja dan Anggaran AAU sampai dengan TW IV TA. 2025 (2025).

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. SAGE Publications.

Lindblom, C. E. (1959). The science of "muddling through". *Public Administration Review, 19*(2), 79–88. https://doi.org/10.2307/973677

Lufti, A. (2022). *Mutu pelayanan pendidikan berbasis e-learning di Akademi Militer* [Master's thesis, Universitas Gadjah Mada]. https://etd.repository.ugm.ac.id/penelitian/detail/208754

Markas Besar TNI. (2019). *Keputusan Panglima TNI Nomor Kep/545/V/2019 tentang Peningkatan Kualitas Pendidikan Militer*. https://tni.mil.id

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

National Institute of Standards and Technology. (2020). *Workforce framework for cybersecurity (NICE Framework)* [NIST Special Publication 800-181 Rev. 1]. https://doi.org/10.6028/NIST.SP.800-181r1

Ornstein, A. C., & Hunkins, F. P. (2018). *Curriculum: Foundations, principles, and issues* (7th ed.). Pearson.

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research, 34*(5 Pt 2), 1189–1208.

Patton, M. Q. (2015). *Qualitative research and evaluation methods* (4th ed.). SAGE Publications.

Publico, M., Tayaban, J. P., Mangalus, A. F., & Arnaldo, R. (2026). Integration of national security interests in select military education institutions' curricula. *The International Review of Multidisciplinary Research, 1*(5), 113–123. https://doi.org/10.5281/zenodo.20184588

Redecker, C., & Punie, Y. (2017). *European framework for the digital competence of educators: DigCompEdu*. Publications Office of the European Union. https://doi.org/10.2760/159770

Setiawan, C. D., Juliherman, J., & Achsyan, D. (2025). Pengembangan kurikulum pendidikan militer berbasis kompetensi digital untuk mendukung interoperabilitas operasi gabungan. *JIIP - Jurnal Ilmiah Ilmu Pendidikan, 8*(11), 12606–12610. https://doi.org/10.54371/jiip.v8i11.9727

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Stufflebeam, D. L. (2003). The CIPP model for evaluation. In T. Kellaghan & D. L. Stufflebeam (Eds.), *International handbook of educational evaluation* (pp. 31–62). Springer.

Stufflebeam, D. L., & Zhang, G. (2017). *The CIPP evaluation model: How to evaluate for improvement and accountability*. Guilford Press.

Surat Telegram Panglima TNI Nomor ST/239/2025 tentang Pengurangan Waktu Pendidikan TA 2025 (2025).

TNI AU. (2021). *Peraturan Kepala Staf Angkatan Udara Nomor 3 Tahun 2021 tentang Grand Strategi Pembangunan Kekuatan AU 2020–2024*. https://tni-au.mil.id

Wahrobun, W., Rufi'i, H., & Muhyi, M. (2019). The policy of curriculum development in education management for cadet of Indonesian Naval Academy. *Journal ASRO, 10*(3). https://doi.org/10.37875/asro.v10i3.146

Weihrich, H. (1982). The TOWS matrix—A tool for situational analysis. *Long Range Planning, 15*(2), 54–66. https://doi.org/10.1016/0024-6301(82)90120-0

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.