Journal of Computer Science

Research Article

Enhancing Sistem Komunikasi Markas (Siskomma) in IS/IT Architecture Planning to Face Modern Warfare: A TOGAF-Based Approach for National Defense Data Integration in the Indonesian Army

Yosua Dwimaryanto Budi Prawiro and Nilo Legowo

School of Information System, Bina Nusantara University, Indonesia

Article history
Received: 23-12-2024
Revised: 16-02-2025
Accepted: 24-02-2025

Corresponding Author:
Yosua Dwimaryanto Budi Prawiro
Information System Management,
Binus University, Indonesia
Email: yosua.prawiro@binus.ac.id

Abstract: In the era of modern warfare, effective Information Systems (IS) and Information Technology (IT) architecture planning are essential for the Indonesian Army to maintain a competitive edge. This paper presents a comprehensive approach to IS/IT architecture planning, focusing on integrating national defense data within the Indonesian Army organization. Utilizing the TOGAF (The Open Group Architecture Framework) approach, the research aligns strategic objectives with operational requirements. Through a detailed assessment of the current landscape, including internal and external factors and strategic goals, this study develops a robust IS/IT architecture plan aimed at enhancing decision-making, operational efficiency, and readiness in facing modern warfare challenges that aligned with the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) function. The research emphasizes that, in facing modern warfare situations, soldiers must first transform themselves into modern soldiers by operating within a modern daily service environment. Introduction and adaptation to technology embedded in daily activity-based service life at the base is a critical element addressed through the scope of the Headquarters Communication System (Sistem Komunikasi Markas - Siskomma) design. This system is one of the four major components of the Indonesian Army Communication and Electronics System (Sistem Komunikasi dan Elektronika - Siskomlek), which forms the core IS/IT architecture of the Indonesian Army. The proposed approach offers a systematic and holistic framework for IS/IT architecture planning in the Indonesian Army, potentially serving as a model for other military organizations confronting similar challenges.

Keywords: Architecture Planning, Modern Warfare, National Defense Data Integration, Indonesian Army, TOGAF, Siskomma, Siskomlek

Introduction

In the contemporary landscape of military operations, the effective utilization of Information Systems (IS) and Information Technology (IT) is paramount for ensuring the readiness and effectiveness of armed forces. Particularly, in the context of the Indonesian Army, the need for robust IS/IT architecture planning to confront modern warfare challenges is critical besides the fact that this military organization is the largest in Indonesia, with almost 400,000 personnel (Jo *et al.*, 2023). This paper focuses on proposing a comprehensive IS/IT architecture planning approach that specifically addresses the integration of national defense data within the Indonesian Army organization. By leveraging the TOGAF (The Open Group Architecture Framework) (TOGAF, 2011) methodology which is a continuation of the Zachman Framework (Zachman, 2003), this research aims to develop a strategic framework that aligns IS/IT architecture with the strategic objectives and operational requirements of the Indonesian Army.

The foundation of enterprise architecture planning can be traced back to the pioneering work of John Zachman, who introduced the Zachman Framework for Enterprise Architecture in 1987 and later refined it in 2003. Some real-world, especially an examples in the military use of the Zachman framework include its initial

implementation in the Department of Defense Architecture Framework (DoDAF) for the US defense system. This framework provided a structured way to understand and classify the various components of an enterprise system by addressing the "what, how, where, who, when, and why" dimensions across different stakeholder perspectives. While the Zachman Framework laid critical theoretical groundwork by offering a taxonomy for organizing architectural artifacts, its lack of process orientation led many organizations to seek a more methodologically driven approach. Over time, this shift in need catalyzed the adoption of TOGAF (The Open Group Architecture Framework), which integrated structured methods, tools, and governance models to guide the development, implementation, and maintenance of EA. TOGAF's Architecture Development Method (ADM) offered a practical roadmap from vision to execution, making it more suitable for large-scale, complex institutions such as defense organizations. This evolution reflects the practical demand for frameworks that not only define architecture components but also provide actionable strategies to align IT infrastructure with organizational goals. Consequently, TOGAF has become the preferred standard in contemporary enterprise architecture planning, including within modern military also in the term of modern warfare contexts such as the Indonesian Army, where this study is situated.

Modern warfare is characterized by rapid technological advancements, increased reliance on data-driven decision-making, and the need for seamless information exchange across various military functions (Laksmana *et al.*, 2020). In this context, the integration of national defense data becomes imperative to enhance situational awareness, optimize resource allocation, and improve overall operational efficiency with the fully support of the first class build quality hardware and software which expected to have the ability to communicate without any interferences, ability to easily support the interoperability requirements inside the Indonesia Army organization without any lack or problem by following the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) function. It is a must, because of its critical stand point as this technology will be the main vital point of the Indonesia Army to operating and orchestrating all of the military personnel, defense equipment, with all the supporting resources behind it. However, achieving this integration poses several challenges, including the complexity of existing IS/IT infrastructure, interoperability issues, and the need for a coherent strategic framework.

The TOGAF approach offers a structured and systematic methodology for addressing these challenges by providing a holistic view of IS/IT architecture planning. The TOGAF method is also one of the options used because based on the literature study obtained, the Architecture Framework in the example of the Army which is already very well established in implementing its technology, such as in the case of the US Army, has used this TOGAF framework from the start, which later became the forerunner of DODAF (Department of Defense Architecture Framework) which is still in use today.By following the TOGAF methodology, this research aims to analyze the current IS/IT landscape of the Indonesian Army, identify key strategic goals and operational requirements, and develop a comprehensive IS/IT architecture plan that integrates national defense data. This plan will not only enhance the Indonesian Army's capability to confront modern warfare challenges but also serve as a model for other military organizations facing similar challenges.

Despite the critical importance of IS/IT architecture planning in modern warfare, the Indonesian Army has yet to fully leverage this approach to enhance its readiness and operational effectiveness. The current IS/IT infrastructure within the Indonesian Army is characterized by disparate systems, lack of interoperability, and limited integration of national defense data. This fragmented approach hinders the Army's ability to effectively harness the power of information and technology in confronting modern warfare challenges. Therefore, there is an urgent need for the Indonesian Army to adopt a systematic IS/IT architecture planning approach, such as the TOGAF methodology, to streamline its IS/IT infrastructure, improve data integration capabilities, and enhance overall operational readiness. By doing so, the Indonesian Army can better prepare itself to address the complexities of modern warfare and ensure the security and sovereignty of the nation.

Furthermore, based on personal observations, there has been a concerning trend within the Indonesian Army (TNI AD) where the adoption of technology has not kept pace with advancements seen in other military organizations globally. This situation has led to a significant gap in the utilization of the latest military technologies, causing the Indonesian Army to lag behind its counterparts in developed countries, such as the United States, the United Kingdom, and other European nations, many of which are members of NATO. This lag in technology adoption has the potential to impact the Indonesian Army's readiness and effectiveness in modern warfare scenarios, highlighting the urgent need for comprehensive IS/IT architecture planning to bridge this technological gap and enhance the Army's capabilities.

Overall, this research contributes to the existing body of knowledge on IS/IT architecture planning in military organizations by providing a practical and strategic approach to address the unique challenges posed by modern warfare. Through the integration of national defense data using the TOGAF methodology, the

Indonesian Army can enhance its operational effectiveness, improve decision-making processes, and ultimately, ensure national security in the face of evolving threats.

Materials and Methods

Literature Review

This research was carried out inseparable from the results of previous studies that had been carried out as study material for the author. To support the research conducted by the author, the author uses several research references from several authors who discuss enterprise architecture using TOGAF. This writing reference was chosen because of its similarities to the writing of the written work that was written. The following is some research that is a reference source for writing papers:

Enterprise Architecture as a Tool in Military Change Management

An exploration of the dynamic nature of a military organization is carried out using qualitative research and evolutionary theory (Mattila, 2018). This journal combines five studies to create a coherent EA model, combining knowledge, information, and information security management at the ICT infrastructure layer. This model was tested in three different Armed Forces transformation journeys, then assessed its validity in determining the positive and negative forces influencing transformation and providing suggestions for change management. The EA model used aims to assist architecture in military organizations in examining existing conditions at this time and finding realistic transformation paths. In this research, the using of Lewin's theory about unfreeze, move, and refreeze as the part of the Change Management has been implented very well. The result show group of analyst as participant can do the as-is and to-be analysis with the success rate of nearly 70% which focus in C4I (Command, Control, Computers, Communications, and Information) and ERP area. The result shown that proposed EA model later can help the military architect to better knowing the change, strength for evolution for the purpose of Transformation Management. Therefore, as the approach of this research only use the C4I aspect and less using of another Architecture Framework, make this research need to find another existing references military Architecture Framework to be taken for sample.

Architecture Frameworks such as DoD, MODAF, and NATO Architecture Frameworks continue to evolve, making it difficult to match metamodels and concepts across paths (Hause *et al.*, 2017). The NATO Architecture Capability Team committed to a single global architecture framework in 2012, resulting in the development of the UPDM V3.0 domain metamodel. This new framework, derived from the MODEM and DoDAF 2.0 metamodels, aims to unify disparate architectural frameworks. This paper will discuss the rationale behind UPDM 3.0 and its new name, Unified Architecture Framework (UAF). An important point in this study is the fact that developed countries such as the United States (US) and the United Kingdom, whose military architecture frameworks are used as the main references in this study, namely DoDAF and MoDAF (NATO Architecture Framework - NAF, not included as a comparison because Indonesia does not have and does not join any military alliance), over the past 10 years have been trying to combine and integrate their Architecture Frameworks, which has manifested in the emergence of the term UPDM (Unified Profile for DoDAF and MoDAF), as well as the UAF (Unified Architecture Framework) concept which thinks further and deeper, namely how DoDAF belonging to the US, MoDAF belonging to the UK, can then be interconnected through interoperability functions with NATO's NAF framework as well as with other coalitions of countries (AGATE belonging to France, DNDAF belonging to Canada, MDAF belonging to Italy, and AusDAF belonging to Australia as well as other Military Architecture Frameworks belonging to NATO member countries that may not yet have been named).

The main challenge is how the Indonesian Army, which is still firmly guided by the principles of the Non-Aligned Movement, can survive the Digital Technology Transformation process that will be structured through the Architecture Framework concept in this research.

The insights gained from the UPDM and UAF concepts from the research conducted by Hause and his colleagues will be invaluable in exploring the crucial points that need to be compiled in developing an Architecture Framework for the Indonesian Army, which still has to fight on its own without any alliances, but does not rule out the possibility of interoperability with this system in the future, in addition to its effective use for internal operations between services (Army, Navy, and Air Force) but can also be integrated with systems used by other countries. As we know, at the ASEAN regional level alone, no military alliance has ever been formed.

The article in the Strategic Corporal, the Tactical General, and the Digital Coup d'oeil – Military Decision-Making and Organizational Competences in Future Military Operations explores the impact of digitalization and knowledge technologies such as the Internet of Things, Big Data, and AI on their impact on military organizations and exercises (Bollmann and Heltberg, 2023). It discusses changes in data generation, analysis, and application, as well as the relationship between these technologies and the concept of Multi-Domain Operations. It proposes new concepts, Digital Mission Command and also digital coup, to navigate the future technological landscape. The interesting things in this research are we are directed to going back to the use of the terminology of three levels of war which is are the

basic grouping in military : tactical, operational, and strategic with the changing the nature of operational art. This research also give a comprehensive bridging to discuss about the C4ISR (minus the another C for Cyber in the C5ISR) function which is also used as one of the pillars in the context of the research on the Architecture Framework for the Indonesian Army. Later will be discussed about the current digital and techological developments (IoT, Big Data, AI), together with the capabilities of these things that can influencing the military organization and command. The other thing is how all of these sophisticated technology also can make a disruptions impact on the existing military concepts. These two things, make a inspiration to develop the latest technology trend to be implemented in the Indonesia Army at the same time by anticipating so that there is no disruption that can backfire on the military organization itself. Datafication, which is at the center of the strategic digitization process discussed in this research, is a crucial technological milestone that marks an era of change in the evolution of a military organization.

Digitilisation, Restrategizing, and the Challenges in Military Defence Transformation

NATO and the EU are implementing digital transformation of their defense systems, with NATO adopting its first digital transformation vision and strategy in 2022 and 2023 (Soare, 2023). The EU has subsequently approved the Strategic Implementation Plan for the Digitalization of EU Forces, which integrates cyber effects in military operations and prioritizes digital capabilities under the fourth pillar of their Strategic Compass document. Digital transformation requires socio-technological and organizational changes, which enable multi-domain operations and defense innovation to run smoothly, seamlessly and without obstacles with maximum support from technological infrastructure. Its ambitious scope includes technology, organizational-procedural and human resources pillars, prioritizing data, cloud and cyber security. However, implementation has been hampered by long lead times, procedural challenges, data sovereignty, and lack of investment in digital capabilities.

Digital innovation within a military organization faces challenges such as realism, coherence, and effectiveness. To overcome this, a categorical reframing process is needed (Fenema and Soldaat, 2022). The three phases include reflection, shifting framing categories, and frame construction. Furthermore, there are four design paradigms that will improve digitalization: establishing nonpermissive ecosystem practices, separating permissive and nonpermissive practices, combining paradoxes, and prioritizing human communication.

The study in journal about Challenges of the Technology 4.0 and Information Technology Within Total War Strategy Structure examines the impact of information technology on Indonesia's universal war strategy, with a focus on positive and negative impacts (Arief *et al.*, 2021). This research, which uses qualitative phenomenology and secondary data from literature studies, shows that the development of information technology has had positive and negative impacts, thus encouraging adjustments to Indonesia's universal war strategy to strengthen its defense against the potential for total war in the future.

The history of the revolution and Indonesia's national defense system, the Universal People's Defense and Security System, has contributed to Indonesia's position and position on the world stage. However, globalization poses threats to sovereignty, especially during the sixth generation of war. In this journal, the aim of strengthening Sishankamrata (Ryacudu *et al.*, 2021), the foundation of national defense, is discussed in the face of the industrial era 4.0. This research uses qualitative descriptive analysis and literature study with a focus on main components, reserve components and supporting components.

In another side, the fast-moving strategic environment is causing tensions between countries, with the strength of the Armed Forces increasing and threats becoming increasingly multipolar. Indonesia faces increased terrorism, drugs and border disputes due to resource use (Sahary *et al.*, 2023). This research aims to provide input to the leadership of the Indonesian Army regarding personnel development, using direct observation and literature study methods. The development of the TNI Army organization to date is still insufficient to address issues occurring in the strategic environment, threats and organizational needs, thus requiring adjustments in recruitment, education and career development.

Literature Gap Analysis

As a comparation to find a Gap Analysis in this research, a previous research title “Design of Enterprise Architecture Technology In Cybercrime Sub-Directorate Of Special Criminal Research Of Metro Jaya Regional Police Using TOGAF Framework” is used. This research start in a phenomenon with the significantly increasing number of Cyber crime, that causing hundreds of billions of dollars in losses annually. Polda Metro Jaya's Cybercrime Division, or Cybercrime Satellite Office, handles cases related to cyber crime and manages technological devices (Yunus, 2020). To address these challenges, the division needs an IS/IT system. The TOGAF ADM framework helps design a systematic and well-organized enterprise architecture for the division. This will help the division plan for future cybercrime cases, align with government, police, and community expectations, and ensure good planning for future investigations.

DOI: 10.3844/jcssp.2025.1855.1871

Then the second comparation is the IS/IT Strategic Planning at the Ministry of Home Affairs' Data and Data Center uses the TOGAF Enterprise Architecture Framework.. This research was conducted at the Pusdatin, Ministry of Home Affairs of the Republic of Indonesia. The lack of optimal governance for information system implementation, use of information technology and data management is one of the existing problems (Kanz, 2020). A design is needed for the development of IT/IS governance at Pusdatin. This research discusses the process of developing Enterprise Architecture at the Pusdatin, Ministry of Home Affairs of the Republic of Indonesia, and how the analysis of the design results can be used as a reference for developing IT/IS governance for the next few years. The method used in this research is TOGAF ADM. Preliminary phase analysis, vision architecture phase, business architecture phase, system information phase, technology architecture phase, opportunities and solution phase, and migration planning are carried out to describe existing conditions and build target architecture. The data in this research was obtained by conducting interviews and literature studies. The results of this research are in the form of recommended enterprise architecture design proposals, solutions to problems, and an IT roadmap based on the analysis that has been carried out.

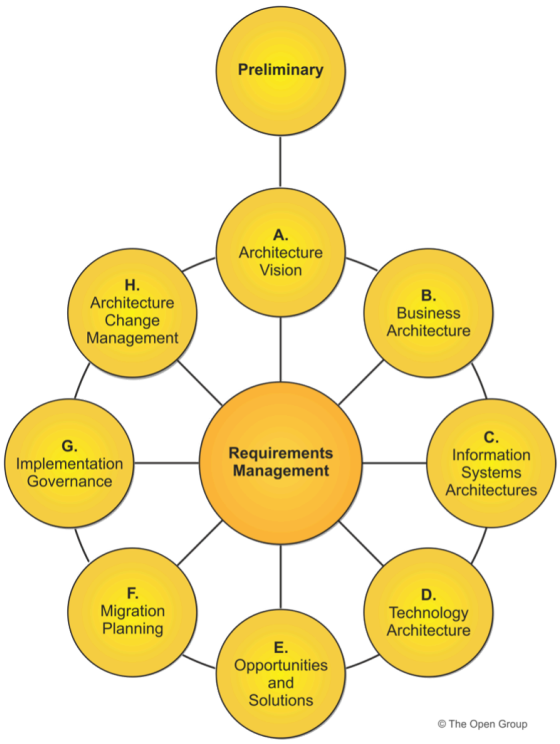

Fig. 1: TOGAF Framework

Methodology

TOGAF Framework

This paper utilizes the TOGAF (The Open Group Architecture Framework) methodology as the primary framework for IS/IT architecture planning in the context of the Indonesian Army's integration of national defense data to face modern warfare challenges. The TOGAF framework, as displayed in Figure 1 is chosen for its comprehensive and systematic approach to developing and managing enterprise architecture.

Phase A: Architecture Vision - The first phase involves establishing the architecture vision, which includes defining the business goals, strategic drivers, and scope of the architecture effort. This phase sets the foundation for the rest of the planning process by aligning the IS/IT architecture with the strategic objectives of the Indonesian Army.

Phase B: Business Architecture - This phase focuses on developing a business architecture that defines the organization's structure, capabilities, and processes. It includes analyzing the current business environment, identifying key business processes, and defining the principles and standards that will guide the IS/IT architecture development.

Phase C: Information Systems Architecture - In this phase, the focus shifts to developing the information systems architecture, which includes defining the data architecture, application architecture, and technology architecture. This phase also involves defining the information flows and interfaces between systems to ensure interoperability and data integration.

Phase D: Technology Architecture - This phase focuses on developing the technology architecture, which includes selecting the hardware, software, and networking components that will support the IS/IT architecture. It also involves defining the technical standards and guidelines that will govern the implementation of the technology infrastructure.

Phase E: Opportunities and Solutions - This phase involves identifying opportunities for enhancing the IS/IT architecture and developing solutions to address them. It includes evaluating alternative architectures and selecting the best approach based on cost, benefits, and feasibility.

Phase F: Migration Planning - This phase focuses on developing a migration plan that outlines the steps required to transition from the current state to the target state architecture. It includes defining the projects, timelines, and resources needed to implement the architecture plan.

Phase G: Implementation Governance - In this phase, the focus is on establishing governance processes to oversee the implementation of the IS/IT architecture. It includes defining roles and responsibilities, establishing monitoring and control mechanisms, and ensuring compliance with the architecture plan.

Phase H: Architecture Change Management - The final phase focuses on managing changes to the IS/IT architecture over time. It includes establishing processes

for evaluating and approving changes, as well as updating the architecture documentation to reflect the changes.

TOGAF framework provides a robust structured and systematic approach to IS/IT architecture planning, ensuring that the Indonesian Army's IS/IT architecture is aligned with its strategic objectives and operational requirements. By following the TOGAF methodology, this research aims to develop a robust IS/IT architecture plan that integrates national defense data and enhances the Indonesian Army's readiness and effectiveness in facing modern warfare challenges.

Field Observations

This paper draws on the author's personal observations and experiences during the service period as a member of the Indonesian Army for at least 10 years that represented on the IS/IT indicator displayed on the Table 1. These observations provide valuable insights into the challenges and opportunities related to IS/IT architecture planning in the context of the Indonesian Army's integration of national defense data to face modern warfare challenges.

Table 1: IS/IT inside Indonesia Army Organization in 2024

IS/IT Indicator	Status	Remarks
IS/IT Architecture	Not Available	Sisfopers, Sisfolog
IS for Organic Military Function	Available	
IS for Special Function	Not Available	
Special/Specific Organization that deals with IS/IT	Available	
Indonesia Army General Staff that focused in IS/IT fields	Not Available	
Use of Indonesia Army Official Email as Official Communication Media	Not Available	
Use of Cloud Storage to support daily administration works	Not Available	
Use of Data-Driven Decision Making (DDDM) to support the Army Services	Not Available	
Use of Business Intelligence as Data Forecasting function to support Army Services	Not Available	
Use of Official IS/IT devices (hardware, software, and other IT infrastructures) that already integrated profesionally	Not Available	

Data Collection - The author's personal observations and experiences, also from doing an interview with selected officer and held a Focus Group Discussion are collected through reflective practice and self-assessment during their service period in the Indonesian Army. These observations are based on direct involvement in various military operations, training exercises, and administrative tasks that require the use of IS/IT systems and technologies.

Analysis - The author's personal observations are analyzed to identify key trends, challenges, and opportunities related to IS/IT architecture planning in the Indonesian Army. This analysis is based on the author's firsthand experiences and insights into the Army's organizational structure, operational processes, and technological capabilities.

Comparison with Literature - The author's personal observations are compared with existing literature and research on IS/IT architecture planning in military organizations. This comparison helps to validate the author's observations and provides a broader context for understanding the challenges and opportunities faced by the Indonesian Army in this regard.

Recommendations - Based on the analysis of personal observations and comparison with existing literature, the author also provides recommendations for improving IS/IT architecture planning in the Indonesian Army. These recommendations are informed by the author's firsthand experiences and aim to address the identified challenges and capitalize on the opportunities identified during their service period.

Previous Works

This paper employs a case study approach to compare the concepts of Information Systems/Information Technology (IS/IT) architecture in the context of defense organizations, focusing on the Defense Architecture Framework (DODAF) used by the United States Department of Defense (DOD) and the NATO Architecture Framework (NAF) used by the North Atlantic Treaty Organization (NATO). The case study involves a comparative analysis of these frameworks to provide insights into their structure, methodology, and effectiveness in supporting defense organizations' IS/IT architecture planning.

- Selection of Case Studies - Examples of case studies are selected from both abroad and within the country. From abroad, the case studies selected for this research are the DODAF used by the DOD and the NAF used by NATO. These frameworks are chosen due to their prominence in the field of defense architecture and their relevance to the Indonesian Army's efforts to enhance its IS/IT architecture planning. Meanwhile, within the country, there are a reference to a previous article by Widodo Swiyadi from University of Indonesia in 2018, titled "Designing Operational Architecture and Application Architecture in Enterprise Architecture for the Military Domain: Case Study of TNI AD Headquarters." Swiyadi's research provides valuable insights into enterprise architecture for the military domain, specifically focusing on the Indonesian Army (TNI AD) Headquarters (Swiyadi, 2018). By referencing Swiyadi's work, this paper aims to build upon his findings and extend the discussion to include a comparative analysis of the DODAF and NAF frameworks.
- Data Collection - Data for the case studies is collected through a review of official documents,

publications, and guidelines related to the DODAF and NAF. This includes documentation provided by the DOD and NATO, as well as scholarly articles and research papers that discuss these frameworks in the context of defense architecture.

- Analysis - The data collected for the case studies is analyzed to identify key similarities and differences between the DODAF and NAF. This analysis focuses on their structure, methodology, key concepts, and the extent to which they support effective IS/IT architecture planning in defense organizations.
- Comparison - The analysis of the case studies involves a comparative assessment of the DODAF and NAF in terms of their strengths, weaknesses, opportunities, and threats (SWOT analysis). This comparison aims to highlight the unique features of each framework and their implications for IS/IT architecture planning in defense organizations.
- Synthesis - Based on the comparative analysis, the paper synthesizes the findings to draw conclusions about the effectiveness of the existing DODAF and NAF in supporting IS/IT architecture planning in defense organizations. The synthesis also includes recommendations for improving IS/IT architecture planning in the Indonesian Army based on lessons learned from the DODAF and NAF.

These case study approach provides a structured and systematic method for comparing the concepts of IS/IT architecture in defense organizations, using the DODAF and NAF as examples. By comparing these frameworks, this research aims to identify best practices and lessons learned that can inform the Indonesian Army's efforts to enhance its IS/IT architecture planning and readiness for modern warfare challenges.

Aligning Attempt With the Recently Indonesian Army's Signal Corps Strategic Plan

Organizational dynamics in the form of the placement of new officials to occupy one of the strategic positions in the Indonesian Army's Signal Center unit also sharpens the final target of the data integration concept which is currently being implemented with the ongoing and the latest urgency needs inside the Indonesian Army organization. In this case, the biggest driving factor comes from three main figures, namely a high-ranking officers with the rank of Major General as the top leader, a Brigadier General as the Signal Branch Director and a middle-ranking officer with the rank of Colonel who is one of the heads of sub-directorates in this main ICT corps unit in the Indonesian Army that has a very vital role for the branch where both have visionary abilities. Which in terms of time momentum has very precise timing with the implementation of this thesis topic.

Continuing what is strategic planning with the TNI Army doctrine, the current leadership then includes the next important points which are based on the Basic Guidelines on 2013 for the Indonesian Army Signal Branches where there are points regarding Communication System building which consists of 4 main aspects which will be the core of the discussion in the organizations, namely the concepts of Siskomma (Sistem Komunikasi Markas), Siskomwil (Sistem Komunikasi Wilayah), Siskomops (Sistem Komunikasi Operasi), and Siskomsus (Sistem Komunikasi Khusus). This concept is currently called Siskomlek (Sistem Komunikasi dan Elektronika) / Communications and Electronic System.

The communications system itself consists of integrated communication networks and technically is an arrangement of tools, equipment, skills, techniques and procedures in the field of communications that are needed to maintain and ensure the continuity of C2 (Command and Control) , operations, organizational activities and other weapons systems.

Meanwhile, Siskomma (Headquarters Communications System) is an orderly totality of all Communication systems and activities prepared at a Command Headquarters in order to carry out the tasks and functions of C2 (Command and Control) and the other Unitary Administration. Siskomwil (Regional Communication System) is an orderly totality of all Communication systems and activities prepared throughout the National Territory within the framework of Hannas/Pertahanan Nasional (National Defence). Siskomops (Operations Communication System) is an orderly totality of all Communication systems and activities that are prepared for unity in the context of implementing Operations. The latest, is Siskomsus (Special Communication System), as an organized totality of all Communication systems and activities prepared in the context of special tasks.

Results and Discussion

Overview of IS/IT Architecture Planning in the Indonesian Army

Research on IS/IT architecture planning for integrating national defense data into the Indonesian Army's infrastructure has revealed significant gaps, particularly due to a lack of accommodation from stakeholders within the TNI Organization. The Army is responsible for IS/IT architecture development, and implementing IT architecture in each function is crucial for the technological era in future years.

The Indonesian Army's Information System development focuses on organic military functions, including existing systems like Sisfopers, Sisfoops, Sisfolog, and Sisforen. Four new Information Systems related to organic military functions are currently supported and running.

The analysis presented in the paper immediately following Table 2 reveals a significant finding: the

DOI: 10.3844/jcssp.2025.1855.1871

current IS/IT architectures in the TNI Army organization are inadequate for military technical functions. The table explicitly shows that IS are Not Exist in the majority of the listed functions, including Main Function, Special Military Technical Function, Special Technical Function, Development Function, Special Function, and General Military Technical Function. This deficiency is particularly noted for the fifteen branches that represent the military technical functions.

Table 2: Existing Condition of Information Systems use in the Indonesia Army Function based on the Doctrine in 2024

Function	Status
Main Function	Non-existent
Special Military Technical Function	Non-existent
Military Organic Function	Exist
Special Technical Function	Non-existent
Development Function	Non-existent
Special Function	Non-existent
General Military Technical Function	Non-existent

Conversely, the table indicates that IS Exist within the Military Organic Function. The research further elaborates that the Indonesian Army's Information System development primarily focuses on these organic military functions, citing examples of existing systems like Sisfopers, Sisfoops, Sisfolog, and Sisforen. Additionally, four new Information Systems related to organic military functions are currently supported and running.

These gaps, clearly illustrated by the numerous "Not Exist" entries in Table 2, are critical infrastructure deficiencies that require immediate attention to improve efficiency and operational effectiveness. The research emphasizes that integrating national defense data into the IS/IT architecture is vital to support all aspects of TNI Army operations, implying that the current state depicted in Table 2 where most functions lack IS is a major hurdle.

Ultimately, the condition shown in Table 2 serves as a foundation for the study's recommendations. It justifies the need for improving the existing IS/IT architecture and highlights areas that require development, such as focusing on a general military technical function information system within units like the Center TNI Army Communications. The proposed IS/IT Future Development Plan uses SISFOHUB as a pioneer-project to address these gaps. The lack of IS implementation across many crucial functions underscores the paper's argument that the Indonesian Army needs to adopt a systematic IS/IT architecture planning approach like TOGAF to streamline infrastructure and enhance operational readiness.

Analysis of Current IS/IT Landscape and Gaps

The study reveals that the current IS/IT architectures in the TNI Army organization are inadequate for military technical functions, with fifteen branches representing these functions. These gaps highlight critical infrastructure deficiencies and require immediate attention to improve efficiency and operational effectiveness. The research emphasizes the importance of integrating national defense data into IS/IT architecture to support all aspects of TNI Army operations.

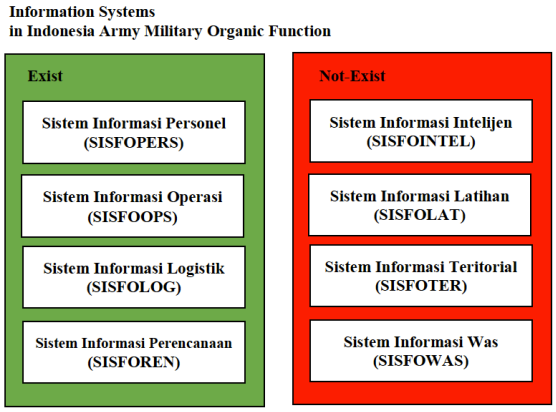

Fig. 2: Existing and Not Existing Condition Diagram in Indonesia Army Military Organic Doctrine

This study recommends improving the existing IS/IT architecture for the Indonesian Army's seven functions, focusing on the development of the SISFOHUB/SISKOMLEK information systems as part of the Military Organic Function. The study will focus on the Central Executive (Balakpus) TNI Army Headquarters, specifically the Center TNI Army Communications, to build a general military technical function information system.

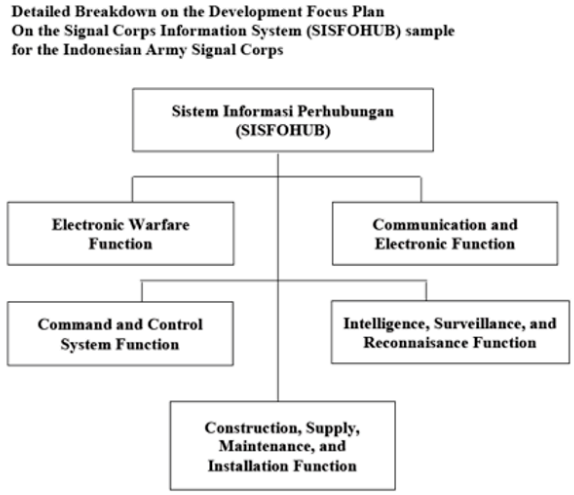

Fig. 3: IS/IT Future Development Plan in Indonesia Army, using SISFOHUB as a pioneer-project

The recommendations include changes and improvements specific to better accommodate the needs of the Indonesian Army, especially regarding data integration for National Defense. By implementing these recommendations, the Army can improve its operational

DOI: 10.3844/jcssp.2025.1855.1871

capabilities and ensure that the IS/IT infrastructure is aligned with its strategic objectives.

This research emphasizes the significance of aligning IS/IT architecture plans with the Army's strategic objectives, enhancing its readiness for modern warfare challenges, and providing valuable insights for improving the Indonesian Army's IS/IT infrastructure. To get the final objective which the adoption of technology is to transform services or business (Martin, 2020).

Initiating the National Defense Data Integration Process From Within Headquarters Using Siskomma

The next findings are formed from a combination of conceptions that come from the researcher as one of the TNI Army officers in the organization, along with leaders in the direct line of leadership to describe the breakdown results of Siskomlek as the last four nodes which are the focus (Siskomma, Siskomwil, Siskomops, and Siskomsus).

Comparative Evaluation: TOGAF vs DoDAF vs MoDAF as Defense IS/IT Architecture for the Indonesia Army

So far, the TOGAF Framework has been used as an option to serve as the foundation and pillar of the framework, which also serves as a justification for this study due to the fact that the development of this concept was carried out almost entirely from scratch using a bottom-up model. This is very different from the comparison of the other two frameworks, each of which represents two developed countries and also two countries whose military strength is highly respected, namely the United States with its DoDAF framework reference and the United Kingdom with its MoDAF framework reference, which clearly shows that the development process uses a top-down flow that is very closely related to the militaristic culture, where in all lines, command and orders are generally centralized, given from top to bottom. Ideally, it is like that, but in the Indonesian Army it needs to be viewed from a different perspective.

With its very unique diversity and a country background that is not part of the mainstream of technological innovation, the Indonesian Army must organize and build its defense technology strength and governance in a way that is the opposite of the two developed countries mentioned above, namely, it is made with a bottom-up concept, or the sample is made first from the bottom up, with the hope that after that it will get further attention from military stakeholders up to the TNI commander in chief to obtain further approval.

Based on the provided source material, based on Figures 2 to Figures 5 that visually illustrate the researcher's logical progression in identifying the focus of the paper, starting from the current state of Information Systems (IS) use within the Indonesian Army doctrine and narrowing down to the specific system for detailed analysis. This path demonstrates a movement from a high-level problem identification to a focused, implementable solution.

Fig. 4: Detailed Breakdown in Developing IS Plan about SISFOHUB

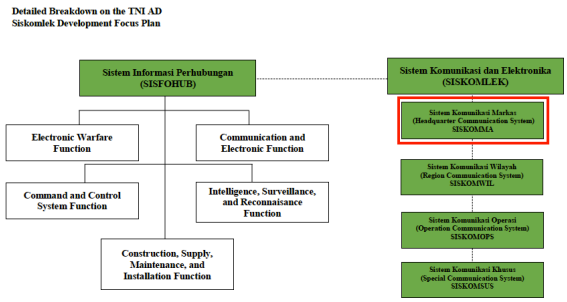

Fig. 5: Detailed Breakdown in Developing IS Plan from SISFOHUB to SISKOMLEK

This analytical path, visually represented by the figures and described in the text, demonstrates how the researcher progressed from a high-level organizational IS/IT assessment to a focused study on a specific, yet critical, component of the Indonesian Army's core communication and electronics system, framed within a broader development plan initiated by a pioneer project concept.

Table 3: Comparative Evaluation TOGAF vs DoDAF vs MoDAF

Feature	TOGAF	DoDAF	MoDAF
Primary Focus	Enterprise architecture across various domains	Military-specific architecture with a strong focus on operational views and data exchange	Defense-focused architecture, emphasizing capability planning and acquisition
Origins	Open Group, vendor-neutral	US Department of Defense	UK Ministry of Defence
Scope	Broad, adaptable to different organizational contexts	Highly specific to military operational needs	Military-specific, aligned with UK defense acquisition processes
Views & Perspectives	Architecture Development Method (ADM) guides the creation of multiple views as needed	Emphasizes operational, systems, and technical views organized within an Operational Architecture, Systems Architecture, and Technical Architecture	Focuses on viewpoints aligned with business, operational, systems, and technical perspectives, supporting capability development
Data & Information Focus	Business-driven, information is a key component	Strong emphasis on data exchange and interoperability between systems	Data is important, but focus is on defining capabilities and their relationships
Method & Process	ADM provides a structured, iterative approach to architecture development	Prescriptive approach with mandated views and products	Flexible approach with guidance on defining viewpoints and conducting analysis
Strengths	Vendor-neutral, widely adopted, adaptable, strong focus on business alignment	Mature framework, proven in large-scale military deployments, strong support for interoperability	Capability-driven, aligns with defense acquisition lifecycle, supports complex stakeholder management
Weaknesses	Can be complex to implement, requires tailoring, less emphasis on specific military needs	Can be bureaucratic and documentation-heavy, less flexible for non-DoD contexts	Less widely adopted outside the UK, may require significant tailoring for different military contexts
Suitability for Indonesia Army	Potentially suitable if tailored to address specific military needs and integrated with existing processes	Less suitable due to US-centric focus and potential compatibility issues with non-US systems	Potentially suitable if Indonesian Army follows a similar acquisition process as the UK MoD, but requires careful adaptation

The following table shows the comparative analysis data between TOGAF, DoDAF, and MoDAF. DoDAF and MoDAF are used as two main references that are analyzed from the perspective of primary focus, origins, scope, views & perspectives, data & information focus, method & process, strengths, weaknesses, and the suitability for the Indonesian Army.

The analytical discussion in the paper following this Table 3, provides the rationale for ultimately selecting TOGAF as the foundational framework for the research. Despite DoDAF and MoDAF being mature, military-specific frameworks, their development followed a top-down flow, which is typical of militaristic cultures where commands are centralized. However, the paper argues that the Indonesian Army, with its unique diversity and background, needs to build its defense technology strength and governance using a bottom-up concept.

While DoDAF and MoDAF are established military architecture frameworks, Table 3 and the subsequent analysis reveal that their prescriptive, top-down, and country-specific nature makes them less suitable for the Indonesian Army's specific context, which necessitates a bottom-up development approach and aligns with a neutral political stance. TOGAF, with its adaptability, openness, and structured but flexible ADM, is identified as the potentially suitable framework that can be tailored to meet these unique requirements.

There are some points to explain the rational strength points to choosing TOGAF as the framework in this research such as the adaptability and opennes, Business-Mission alignment, ADM as a guide, and integration with the existing standards.

Intelligence viewpoints in purposes to incorporating intelligence-specific requirements and data flows, Joint operations viewpoints that consists of addressing interoperability with other branches of the Indonesian military and friendly country with a good diplomatic regional/bilateral relation and Teritorial Defenses viewpoints are the objectives to overcome the adaptability and openness as the TOGAF are in the clear area to state that Indonesia are remain neutral from not using other country framework that can lead opinion to involvement and alignment with certain alliances.

Another TOGAF's focus is to aligning ICT inside the Indonesia Army Organization with business goals are the highlight point . This will later explain how this translates to supporting the Indonesian Army's strategic objectives, such as modernization, improved readiness, and enhanced capabilities.

ADM as a guide will explain how the ADM provides a structured process for developing and managing architecture, ensuring consistency, and completeness. For the last consideration is the integration with existing standards which then it will emphasize the importance of selecting and using the TOGAF framework in this study to later discuss how TOGAF can be integrated with relevant Indonesian military standards and regulations.

The independence and freedom in choosing, building, developing, and using the framework provided by The Open Group in this open form Framework (TOGAF), which can be used by anyone, including the Indonesian Army will be a special case that in conclusion, this Framework is gonna be align with the Indonesia National Politics stand point, which is to remain neutral country (Non-Aligned Movement/NAM).

Application of the TOGAF Framework in Defense IS/IT Architecture Framework

TOGAF was chosen for its comprehensive, phased approach that ensures alignment between IS/IT systems and the strategic and operational objectives of defense organizations. By following TOGAF's Architecture Development Method (ADM), the research systematically progressed from defining an overarching architecture vision to creating detailed designs for business, data, application, and technology architectures. Each TOGAF phase—such as Architecture Vision, Business Architecture, Information Systems Architecture, and Technology Architecture—was applied to develop a cohesive framework. This approach provided a structured pathway for addressing current gaps, ensuring interoperability, and integrating national defense data, thereby enhancing the Army's operational effectiveness and readiness for modern warfare challenges.

After completed the Preliminary Phase, which include Establishing the Architecture Framework and Principles to Make a Risk Assesment and Mitigation Planning, then the following phase is how the TOGAF Framework is implemented in detail, accompanied by an explanation of the process for each existing stage in this research.

Phase A: Architecture Vision. The initial phase involved establishing a clear vision for the architecture, defining strategic objectives, key drivers, and scope of the IS/IT architecture for the Indonesian Army. Here, the goals of enhancing data integration, interoperability, and readiness for modern warfare were prioritized, setting a foundation that guided all subsequent phases. This phase also aligned the IS/IT architecture plan with the Indonesian Army's broader mission, ensuring that the architecture supported the organizational vision.

Phase B: Business Architecture. In this phase, the focus was on understanding and documenting the existing organizational structure, processes, and key capabilities within the Army. Business functions were mapped, and core requirements for IS/IT support were identified, particularly in terms of communication, decision-making, and operational coordination. This phase helped clarify the role of each function within the Army, ensuring that the IS/IT architecture would support core business activities effectively.

Phase C: Information Systems Architecture. The Information Systems Architecture phase defined the essential data and application structures required for effective defense operations. This involved designing data flows, system interfaces, and applications to enable seamless data exchange across different functions. Key systems were identified and outlined to ensure they could support the requirements for national defense data integration, improving real-time access to critical information and enhancing operational coordination.

Phase D: Technology Architecture. The Technology Architecture phase focused on selecting and structuring the necessary hardware, software, and network infrastructure to support the information systems architecture. This included defining technical standards, such as interoperability protocols and security requirements, and selecting technologies suited to the defense environment. The result was a resilient and secure infrastructure design that could handle the demands of national defense data while ensuring robust protection against cyber threats.

Phase E: Opportunities and Solutions. During this phase, potential improvements to the IS/IT architecture were explored, including evaluating alternative architectures and identifying specific solutions to address current gaps. The focus was on finding cost-effective, scalable options that met the strategic requirements. Several architecture options were analyzed based on factors such as cost, feasibility, and alignment with Army priorities, ensuring the most practical solutions were chosen.

Phase F: Migration Planning. This phase involved creating a detailed migration plan to transition from the current state to the envisioned target architecture. Timelines, resources, and project milestones were outlined, along with a phased implementation strategy to ensure a smooth transition with minimal operational disruption. Migration planning included detailed steps for data integration, system upgrades, and workforce training.

Phase G: Implementation Governance. TOGAF's Implementation Governance phase established processes for overseeing and monitoring the IS/IT architecture implementation. Roles and responsibilities were clearly defined, and mechanisms for tracking progress and ensuring compliance with the architecture plan were introduced. This governance framework ensured alignment with strategic objectives throughout the implementation, while also allowing for adjustments as needed.

Phase H: Architecture Change Management. The final phase addressed the need for ongoing management and adaptation of the architecture to respond to new requirements or operational challenges. Change management processes were put in place to assess and integrate updates to the architecture, ensuring that the IS/IT framework remained responsive and relevant to evolving defense needs over time.

By applying TOGAF across these phases, the research achieved a structured, strategic approach to IS/IT planning that aligned the Indonesian Army's technological infrastructure with its operational and strategic objectives. This approach not only addressed immediate architecture needs but also laid the groundwork for future adaptability and continuous improvement, strengthening the Army's readiness and resilience in the face of modern warfare challenges.

DOI: 10.3844/jcssp.2025.1855.1871

Table 5: Detailed Plan in Siskomma Program Feature

Sub Code	Main Program	Prog Code	Program Feature	Description	Technology
SKM-1	Unified Communication	SKM-1.1	Voice System	Use of communication within the headquarters by voice	VoIP, App, HT Radio (VHF, UHF, HF), Office Intercom, Office Telephone, integrated PA system
		SKM-1.2	Email System	Use of official email for all TNI AD soldiers	Mailing System, Server, etc
		SKM-1.3	Video Conference	Internal communication system that serves two-way communication, webinars, discussions, meetings and teleconferences using video	Zoom, TNI AD Alpha Delta Secure Video Conference App, etc
SKM-2	Digital Office	SKM-2.1	Office Business Process Document	A concept for creating living documents that contain digitalization of SOPs, habits, processes, mechanisms that can always be accessed, updated, and maintained.	BPMN (Business Process Model Notation) 2.0 document, Enterprise Content Management (ECM) system, Digital Document Workflow Automation Tools, Cloud-Based Collaboration Platforms, AI-Driven Document Management and Analysis Tools
		SKM-2.2	Digital Document Archiving	Applications and hardware that can convert the flow habits of administrative activities related to scripts	
		SKM-2.3	System Access	a system that regulates authority, access rights, electronic signatures according to position and legality according to regulations	
		SKM-2.4	Integrated and Automated Attendance and Arrival Tracking System	Providing a feature as an army organization's attendance management solution, utilizing IoT, biometric authentication, and GPS tracking. It streamlines processes, provides real-time data, and integrates with HR systems for efficient personnel management.	IoT, biometric authentication, GPS tracking, and cloud-based integration
		SKM-2.4	Integrated Office Submission	A digital platform for managing administrative submissions within an army organization, streamlining essential requests like official leave, sick leave, and financial loan applications. It automates workflows, reduces paperwork, and enhances transparency.	Low-Code/No-Code Development Platforms, Business Process Management and Workflow Automation Tools, Document Management Systems, Cloud Infrastructure and Database Management, API Integration Frameworks, Role-Based Access Control (RBAC) and Security Features) Analytics and Reporting Tools
SKM-3	Enterprise Resource Planning	SKM-3.1	Asset Management	Management of assets belonging to soldiers and units more effectively to achieve effectiveness and efficiency of performance.	SAP EAM (Enterprise Asset Management)
		SKM-3.2	TNI AD Information System Apps	Information System Applications are used to implement several required business processes.	Low-code/no-code platforms for rapid deployment
		SKM-3.3	HQ Security & Maintenance System	A system that controls headquarters governance, headquarters control systems, security, headquarters standard operating procedures digitally.	Oracle Maintenance Cloud, SAP PM
SKM-4	AI Assistance	SKM-4.1	Sergeant Papin (TNI AD AI Assistance)	Sergeant Papin is an AI-based virtual assistant designed to assist in daily TNI AD office tasks and provide quick answers to common army organization questions. It handles scheduling, reminders, and provides knowledge on army services, policies, and protocols.	Natural Languange Processing. Machine Learning, Voice and Chat Integration
		SKM-4.2	AI-Powered TNI AD Letter Drafting Assistant	The AI-Powered Army Letter Drafting Assistant streamlines the drafting, editing, and formatting of official letters in the army office. It automates drafting, follows templates, and aligns content with military protocol, reducing errors and saving time.	NLP for Text Generation and Editing, Grammar and Compliance Tools, Machine Learning Model Training
		SKM-4.3	AI-Powered Personnel Capability Indicator Summary System	The AI-Powered Personnel Capability Summary System is a tool that visually summarizes and assesses the skill and experience profiles of army personnel across 15 branches. It evaluates physical fitness, health, education, and job histories, providing a data-driven overview of strengths and areas for growth.	Data Aggregation and Analysis, Machine Learning Algorithms, Data Visualization for Summary Output, Natural Language Processing for Profile Summarization
SKM-5	Learning and Development	SKM-5.1	TNI AD Learning Management System for Individual Army Personnel	The TNI AD Learning Management System is a platform for army personnel to continuously learn and enhance their skills. It offers military and professional development courses, resources, and interactive training modules, ensuring personnel stay updated with evolving practices.	Moodle, Blackboard, SAP SuccessFactors Learning, or Docebo
		SKM-5.2	VR and AR Simulation Training Platform	The VR and AR Simulation Training Platform is a virtual training system that simulates complex operational scenarios, enhancing soldiers' decision-making, coordination, and tactical skills. It uses VR and AR technologies, real-time performance tracking, and IoT integration for cost-effective, risk-free training.	VR Hardware and Software (Oculus for Business, HTC Vive, or Varjo for VR hardware, combined with VR development platforms like Unity or Unreal Engine for creating immersive simulations) and AR Development Tools (Microsoft HoloLens, Magic Leap, or ARKit (for Apple devices), with development environments in Unity or Unreal Engine)

DOI: 10.3844/jcssp.2025.1855.1871

Design and Functionality of Siskomma Components

Furthermore, due to the existing limitation factors and also with the direction and approval of the upper command in the Army Signal Unit as a policy maker, further discussion in this section will be more directed and focused again only on the Siskomma aspect.

With the instructions obtained from the leadership as relevant stakeholders, several main desires for the desired Siskomma concept were obtained, which are visualized in Table 4.

In the context of IS/IT architecture planning to address modern warfare through the integration of national defense data within the Indonesian Army, one of the four core components of the SISFOHUB feature is the Headquarters Communication System, or Siskomma (SKM). The SKM is meticulously structured into four distinct modules to enhance operational efficiency and strategic capabilities. SKM-1 focuses on Unified Communication, which integrates a comprehensive Voice System, an Email System, and Video Conferencing to ensure seamless and secure communication across all levels of the organization. SKM-2 emphasizes the Digital Office, aimed at creating a digital and paperless office environment. This module includes systems for managing digital documents and access control, streamlining administrative processes, and enhancing operational agility. SKM-3, the Enterprise Resource Planning (ERP) module, encompasses Assets Management, various Indonesia Army Information System Applications, and HQ Maintenance and Security Applications, facilitating the effective management of resources and operational activities. SKM-4 introduces AI Assistance, leveraging artificial intelligence to support decision-making processes and enhance the overall responsiveness of the army's headquarters. Finally, SKM-5 handle the Learning and Development process activity to ensure that all soldiers still can develop their own military knowledge driven by the technology. This comprehensive breakdown of the SKM highlights its pivotal role in strengthening the IS/IT architecture and ensuring the Indonesian Army's preparedness for modern warfare through improved communication, resource management, and technological integration.

The expected Siskomma infrastructure embodies a comprehensive and technologically advanced setup designed to create a smart, modern army office. This infrastructure integrates a variety of digital IoT devices to enhance operational efficiency, security, and communication within the Indonesian Army's headquarters. Key components include CCTV systems for surveillance, ensuring constant monitoring and security. IP Phones provide robust and reliable communication channels, while seamless Wi-Fi internet access ensures uninterrupted connectivity across the office. Door access with smart locks enhances security by allowing only authorized personnel to enter specific areas. Smart displays are strategically placed to provide real-time information and updates. The Office Integrated Public Address Announcement System enables efficient dissemination of important messages. Additionally, the infrastructure includes advanced fire alarm systems, a cooling system for maintaining optimal working conditions, and smart lighting systems to ensure energy efficiency and a comfortable working environment. All these devices can be individually controlled by authorized personnel with access rights, ensuring flexibility and security. Moreover, the building management team (internal affairs) has overall control access, allowing them to manage and monitor the entire system to ensure smooth and efficient operation of the smart army office. This integrated infrastructure significantly enhances the capabilities and preparedness of the Indonesian Army by providing a secure, efficient, and technologically advanced working environment.

The Role of AI in Enhancing Operational Efficiency

The AI technology implementation within the Siskomma (SKM) feature is designed to enhance the operational capabilities and decision-making processes of the Indonesian Army through a range of advanced functionalities. The AI components are visualized in a figure table (see Table IV) that outlines their specific abilities and their integration with various system functions such as the Control Center, Security Information and Event Management (SIEM), System Administration Management (SAM), and Enterprise Resource Planning (ERP). The key AI capabilities include:

- Speech to Text: This feature allows for the conversion of spoken language into written text, facilitating real-time transcription of meetings and communications, which is crucial for the Control Center.
- Text to Speech: This capability enables the system to convert written text into spoken language, enhancing communication efficiency and accessibility within the Control Center and SAM.
- Image/Video Analytics: AI-driven analysis of visual data helps in identifying patterns, anomalies, and threats, supporting SIEM and enhancing surveillance and security measures.
- Document Summarization: AI can summarize lengthy documents, providing concise and relevant information quickly, which is particularly useful for ERP and SAM in managing large volumes of data.
- Translator: This feature provides real-time translation services, breaking down language barriers and enhancing communication within the Control Center and across different units.
- Analytics: Advanced analytics capabilities enable the system to process and analyze vast amounts of data, providing valuable insights for decision-making processes in the Control Center and ERP.

- Prediction: Predictive analytics help in forecasting potential issues and trends, supporting proactive measures in SIEM and ERP.
- Classification: AI can classify and organize data efficiently, aiding in better data management and retrieval in SAM and ERP.
- Decision Support System (DSS): The DSS leverages AI to provide actionable insights and recommendations, enhancing strategic planning and operational decisions in the Control Center and ERP.

These AI functionalities are integrated into the Siskomma feature to support a cohesive and intelligent system, ensuring that the Indonesian Army's headquarters operate with enhanced efficiency, security, and strategic capability. The integration of AI technology into Siskomma exemplifies a forward-thinking approach to modernizing military operations and maintaining a robust defense posture.

A central highlight of this research is the introduction of a smart AI assistance system for all Indonesian Army personnel, named 'Sersan Papin.' (see Figure 6) Derived from the Indonesian words 'Patuh' and 'Pintar,' meaning 'Obedient' and 'Smart,' Sersan Papin represents a significant milestone in enhancing administrative support and service quality within the organization. This sophisticated AI character is designed to provide dedicated service to soldiers, streamlining their daily administrative tasks and improving overall efficiency. Sersan Papin's capabilities include seamless connectivity to the Headquarters Control Center Database, enabling real-time access to crucial information and resources. It also features interactive displays for intuitive and user-friendly interactions, and a Unified Communication AI System that integrates voice, video, and messaging services. These features collectively aim to transform the experience of Indonesian Army personnel, offering a more impressive and profound level of service and support. The implementation of Sersan Papin is expected to set a new standard in military administrative assistance, reflecting a commitment to leveraging advanced technology to enhance operational effectiveness and personnel satisfaction.

Fig. 6: Sersan Papin (Patuh dan Pintar) as an AI Virtual Assistance Feature to support the Siskomma System

Mitigating Risks of AI in Military Systems: A TOGAF Phase F Approach

High consideration already thinked in decision to put an integration of Artificial Intelligence (AI) into this military systems inside the Indonesia Army organization to offers significant potential advantages, for example, from the daily military personnel personal assistance (Sersan Papin-SKM 4.1), a proof read and assistance to do create daily official Army letter (AI-Powered TNI AD Letter Drafting Assistant-SKM 4.2), AI Tools for knowing the capability from the military personnel individual (SKM 4.3), to the function for enhancing situational awareness to automated decision-making. However, this integration also presents substantial risks, particularly concerning bias in AI models and complex ethical considerations. These risks necessitate careful planning and mitigation strategies to ensure responsible and effective deployment. This discussion explores these challenges and proposes a mitigation approach based on Phase F: Migration Planning within the TOGAF framework.

The challenges are the bias in AI models, ethical considerations, lack of transparency and explainability, and about the data security and integrity.

AI models are trained on data, and if this data reflects existing societal biases, the model will perpetuate and potentially amplify them. In a military context, biased algorithms could lead to discriminatory targeting, disproportionate use of force against specific populations, or misinterpretation of threat assessments. This can have severe legal, ethical, and strategic consequences. This will be the main highlight to notice about how bias in AI models will be happening in this implementation of these AI features.

In case of ethical consideratios, AI in military systems raises complex ethical dilemmas. These include questions of accountability (who is responsible for an AI's actions?), autonomy (should AI be allowed to make life-or-death decisions?), and the potential for unintended consequences (e.g., escalation of conflict due to algorithmic miscalculation). The lack of clear ethical guidelines and international legal frameworks creates a challenging landscape. Even the implementation of AI features in this concept are still focused on the daily basic activity (not a combat purpose AI), but the awareness of the personnel of Indonesia Army must be build up from the beginning. These initial daily AI features will help the personnel of Indonesia Army to transform easily and slowly to this new technology environment before another sophisticated AI feature are going more to come.

Another problems to face, that many AI models, particularly deep learning systems, operate as "black boxes." Their decision-making processes are opaque, making it difficult to understand why a particular

DOI: 10.3844/jcssp.2025.1855.1871

outcome was reached. This lack of transparency hinders trust and accountability, especially in critical military applications. This issue later will raise the lack of transaparency and explainability.

Lastly, these military AI systems concept to be implemented in the Indonesia Army are rely on vast amounts of data, making them vulnerable to cyberattacks and data manipulation. Compromised data can lead to skewed models and unreliable outputs, potentially jeopardizing mission success and national security. Data security and integrity must be in a full concern to be always 24/7 monitored by a watchdog system.

Next approach are how to get a Mitigation Approach using TOGAF Phase F (Migration Planning). When this phase focuses on developing a detailed implementation and migration plan for the proposed architecture. Applying this phase to mitigating AI risks in military systems involves the following steps:

1. Risk Assessment and Prioritatization: Conduct a comprehensive risk assessment to identify and prioritize potential AI-related risks. This should involve experts from various disciplines, including AI specialists, ethicists, legal experts, and military personnel. The assessment should consider both technical risks (e.g., model bias, data security) and operational risks (e.g., unintended consequences, loss of human control).
2. Defining Mitigation Strategies: Based on the risk assessment, develop specific mitigation strategies for each identified risk. These strategies might include:
3. Data Diversity and Quality Control: Implement rigorous data governance processes to ensure the training data is diverse, representative, and free from bias. This may involve collecting new data, augmenting existing datasets, and employing techniques like adversarial training to improve model robustness.
4. Explainable AI (XAI) Development: Prioritize the development and use of XAI techniques to enhance the transparency and interpretability of AI models. This will allow for better understanding of decision-making processes and facilitate human oversight.
5. Ethical Guidelines and Frameworks: Establish clear ethical guidelines and frameworks for the development and deployment of military AI systems. These frameworks should address issues of accountability, autonomy, and human control, and should be aligned with international legal norms.
6. Robust Security Measures: Implement robust cybersecurity measures to protect data and AI models from unauthorized access and manipulation. This includes encryption, intrusion detection systems, and regular security audits.
7. Human-in-the-Loop Systems: Maintain human oversight and control over critical AI-driven decisions, especially in Lethal Autonomous Weapons Systems (LAWS). This ensures that human judgment remains central and prevents unintended escalation.
8. Developing a Migration Plan: Create a detailed migration plan that outlines the steps required to implement the mitigation strategies. This plan should include timelines, resource allocation, and responsibilities. It should also address the integration of AI systems with existing military infrastructure and workflows.
9. Testing and Evaluation. Conduct rigorous testing and evaluation of AI systems before deployment. This should include testing for bias, robustness, and ethical compliance. Independent audits and red teaming exercises can help identify vulnerabilities and improve system performance.
10. Monitoring and Continuous Improvement. Establish a continuous monitoring process to track the performance of deployed AI systems and identify any emerging risks. This feedback loop should inform ongoing improvements to the models, data, and mitigation strategies.

Outputs Obtained from the Implementation of the Research

IS/IT Architecture Plan: A comprehensive architecture plan designed to integrate national defense data, guided by the TOGAF framework, to support strategic and operational needs in TNI AD organization.

Siskomma System Design: A detailed plan for implementing the Siskomma (Sistem Komunikasi Markas) communication system. This includes features like unified communication, digital office functionalities, and AI support, all aimed at improving command, control, and coordination within army headquarters.

AI Assistance Integration: The development of an AI-based assistance system (Sersan Papin) to support personnel in administrative and decision-making tasks, enhancing efficiency and service quality.

Operational Infrastructure Recommendations: Proposals for integrating IoT devices, such as CCTV, IP phones, and smart displays, within the headquarters to streamline operational processes and security measures.

Strategic IS/IT Framework Recommendations: Insights and recommendations for aligning IS/IT planning with the Indonesian Army's strategic goals, proposing improvements to current architectures that may also serve as a model for other military organizations.

Conclusion

The Indonesian Army as one of the military organizations with the largest strength in Indonesia with a personnel of approximately 350,000 soldiers and as part of a global force together with other TNI

components which is the 13th largest force in the world (based on data from Global Firepower), is currently in a transition period to be able to grasp its ICT superiority after being quite behind in the adaptation process in the last few periods.

This lag can be proven by the absence of an IS/IT Architecture framework that is specifically created to support the implementation of the duties of the Indonesian Army which is organizationally under the TNI Headquarters and also under the Ministry of Defense.

If we refer to a similar framework such as DoDAF (Department of Defense Architecture Framework) which has been implemented in the United States with a top-down pattern, where the framework is implemented from the U.S. Department of Defense, ideally the Indonesian Ministry of Defense can do the same. However, because in this study various obstacles were found both from technical, cultural, HR, and other aspects, so that the pattern of creating an IS/IT framework leads to a solution to be implemented in a bottom-up manner starting from the Indonesian Army then continuing to the Indonesian Army Headquarters and the Ministry of Defense at the final stage, or the opposite of what was done by the US Department of Defense which implemented a top-down pattern.

In this study, as an outcome, it is generally presented the real concept that has currently become a policy that is being implemented within the Indonesian Army organization with the development of the Siskomlek Architecture which consists of four large parts, namely Siskomma, Siskomwil, Siskomops, and Siskomsus where the discussion of Siskomma is the main core in the detailed discussion in the scope of this research. The other more specific outcome of one of the feature displays of the Information Communication and Electronics System (Sisfokomlek) concept is to answer the daily works problems in the Network section under the Sub Directorate of Communication Development of the Indonesian Army Signal Center that later displayed as an integrated solution with the Siskomma features in general, which has the scope of its duties to be responsible for all deployment of communication networks/backbones within the Indonesian Army organization with the use of several AI technology as the newa features to support daily Indonesia Army tasks.

Successfully integrating AI into the Indonesia Army systems requires a proactive and comprehensive approach to risk management. By leveraging TOGAF Phase F and implementing the mitigation strategies outlined above, Indonesia Army as a modern military organizations can minimize the potential harms of AI and ensure its responsible and ethical use. This requires ongoing collaboration between AI researchers, ethicists, legal experts, military personnel, and involvement of the national stakeholder to navigate the complex challenges posed by this rapidly evolving technology. The focus should always remain on maintaining human control, upholding ethical principles, and ensuring the safety and security of both military personnel and civilians.

This paper then is expected to be a stepping stone in the context of refining all previous research in the scope of developing an Architecture Framework in military organizations and continuing to sow the seeds of technology that will never be separated from the military world itself, because basically the technology that most of us enjoy today is the work of past conflicts. The continuation of research from the discussion of this paper in the future is also no less important to be able to continue continuously and relentlessly.

As a final remarks, a structured IS/IT Architecture Framework technology in the fast pace has become the main driving force in the Indonesian Army Organization. Now and in the years to come, the role and function of technology that manifested in the form of an Architecture Framework will continue to be maximized through organizational management that is more oriented towards the latest technological developments.

Acknowledgment

The authors would like to express their heartfelt gratitude to the leadership and personnel of the Indonesian Army Signal Corps for their unwavering support and guidance throughout this research. Special thanks go to Bina Nusantara University for providing the resources and academic environment necessary to complete this work. The authors are also grateful to their colleagues, fellow soldiers, and peers for their constructive feedback and encouragement.

Funding Information

This research was conducted without any external funding. All efforts and resources were supported by the authors independently.

Author's Contributions

Yosua Dwimaryanto: As an active soldier and researcher in the Indonesian Army, was responsible for collecting and analyzing the data relevant to this study.

Nilo Legowo: As an active lecturer also a senior researcher, provided direction and guidance regarding the selected frameworks, ensuring their alignment with the objectives of IS strategic planning in the defense sector.

Ethics

This research adheres to ethical standards in academic and professional conduct. All data collected and analyzed were obtained with appropriate permissions and in compliance with institutional and organizational guidelines. The authors confirm that no sensitive or classified information was disclosed or compromised during this study.

References

Arief, R., Risman, H., & Sutanto, R. (2021). The Challenges of the Technology 4.0 and Information Technology Within Total War Strategy Structure. *Jurnal Pertahanan: Media Informasi Ttg Kajian and Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity*, *7*(1), 73-88. https://doi.org/10.33172/jp.v7i1.1099

Bollmann, A. T., & Heltberg, T. (2023). The Strategic Corporal, the Tactical General, and the Digital Coup d'oeil - Military Decision-Making and Organizational Competences in Future Military Operations. *Scandinavian Journal of Military Studies*, *6*(1), 151-168. https://doi.org/10.31374/sjms.190

Fenema, P., & Soldaat, P. (2022). *Restrategizing Digitalization in the Military*.

Hause, M., Bleakley, G., & Morkevicius, A. (2017). Technology Update on the Unified Architecture Framework (Uaf). *INSIGHT*, *20*(2), 71-78. https://doi.org/10.1002/inst.12153

Jo, H., Bentham, J., le Breton, C., Decis, H., Dempsey, J., *et al*. (2023). *The Military Balance 2023*. https://doi.org/10.4324/9781003400226

Kanz, A. F. (2020). *Perencanaan Strategis IS/IT di Pusdatin Kemendagri menggunakan Framework Enterprise Architecture TOGAF*.

Laksmana, E. A., Gindarsah, I., & Maharani, C. (2020). 75 tahun TNI: Evolusi Ekonomi Pertahanan, Operasi, dan Organisasi Militer Indonesia. *CSIS Indonesia*.

Lisa, N. P. (2017). Analisis Itensitas Pencahayaan Alami pada Ruang Kuliah Prodi Arsitektur Universitas Malikussaleh. *Temu Ilmiah Ikatan Peneliti Lingkungan Binaan Indonesia 6*. Temu Ilmiah Ikatan Peneliti Lingkungan Binaan Indonesia 6. https://doi.org/10.32315/ti.6.h061

Martin, A. (2020). *Digital Literacy and the "Digital Society" in Digital Literacies: Concepts, Policies, and Practices*. *30*, 151-176.

Mattila, J. (2018). Enterprise Architecture as a Tool in Military Change Management. *Proceedings of the 6th International Conference on Management, Leadership and Governance, ICMLG*.

Ryacudu, R., Putra, I. N., & Purwantoro, S. A. (2021). Strengthening Total People's Defense and Security System iIn The Industrial Revolution Era 4.0 to Face the Threat of Sixth Generation War. *Jurnal Pertahanan: Media Informasi Ttg Kajian AndStrategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity*, *7*(2), 191-204. https://doi.org/10.33172/jp.v7i2.1231

Sahary, F. T., Mutaqin, R., Mutaqin, G., & Dharmopadni, D. S. (2023). Transformation of Indonesian Army Personnel to Produce Experts Soldiers in the Field of Technology. *Jurnal Pertahanan: Media Informasi Ttg Kajian & Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism & Integrity*, *9*(1), 167-177. https://doi.org/10.33172/jp.v9i1.3264

Soare, S. (2023). Digitalisation of defence in NATO and the EU: Making European Defence Fit for the Digital Age. *IISS*.

Swiyadi, W. (2018). Perancangan arsitektur operasional dan arsitektur aplikasi pada enterprise architecture untuk ranah militer: studi kasus Markas Besar TNI AD. *MTI Universitas Indonesia*.

TOGAF. (2011). SO Cloud Computing Infrastructure Framework. *The Open Group*.

Yunus, F. (2023). Perancangan enterprise architecture teknologi pada subdit cybercrime direktorat reserse kriminal khusus polda metro jaya menggunakan TOGAF framework. *Binus MMSI*.

Zachman, J. A. (2003). The Zachman framework for enterprise. *Zachman Int*.