International Journal of Safety and Security Engineering
Vol. 15, No. 12, December, 2025, pp. 2561-2572
Journal homepage: http://iieta.org/journals/ijsse

An Integrated Smart Defense Architecture for the Nusantara Capital City of Indonesia

Muhammad Arsy Ash Shiddiqy[1*], Riky Novarizal[2], Mohd Syaiful Nizam Bin Abu Hassan[3], Dani Kurniawansyah[4], Alficandra[5]

[1] Department of International Relations, Universitas Islam Riau, Pekanbaru 28284, Indonesia
[2] Department of Criminology, Universitas Islam Riau, Pekanbaru 28284, Indonesia
[3] Faculty of Applied Social Sciences, Universiti Sultan Zainal Abidin, Kuala Nerus 21300, Malaysia
[4] Department of Law, Universitas Pasir Pengaraian, Pasir Pengaraian 28558, Indonesia
[5] Department of Physical Education, Universitas Islam Riau, Pekanbaru 28284, Indonesia

Corresponding Author Email: arsyshiddiq@soc.uir.ac.id

https://doi.org/10.18280/ijsse.151213

Received: 13 October 2025
Revised: 14 December 2025
Accepted: 23 December 2025
Available online: 31 December 2025

Keywords:
intelligent defense architecture, national resilience, Nusantara Capital City, public security, technology integration

ABSTRACT

The development of Indonesia's new capital city, the Nusantara Capital City (IKN), requires an integrated defense architecture capable of addressing complex and multidimensional security challenges within a smart city environment. This study aims to design a smart defense architecture that integrates technological security, national resilience, and public security from a safety and security systems engineering perspective. The research adopts a qualitative, document-based approach using secondary data derived from national defense policies, strategic planning documents, and international capital city security cases. A Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis is employed to identify key internal and external defense factors, which are subsequently structured and prioritized using the Analytic Hierarchy Process (AHP). The recalculated AHP results indicate that the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system emerges as the highest-priority component with a weight of 0.466 (46.6%), followed by Artificial Intelligence (AI)-based surveillance at 0.277 (27.7%), digital infrastructure security at 0.161 (16.1%), and inter-agency collaboration at 0.096 (9.6%), with the total weights summing precisely to 1.000 (100%) in accordance with standard AHP normalization procedures. These findings demonstrate the central role of integrated command systems and intelligent technologies in strengthening security governance and national resilience in IKN. The proposed framework provides a structured decision-support model to guide policymakers in developing adaptive, technology-driven, and sustainable defense systems for strategic capital cities.

1. INTRODUCTION

The relocation of Indonesia's national capital, the Nusantara Capital City (IKN) from Jakarta to East Kalimantan, represents a strategic national initiative aimed not only at reducing Jakarta's ecological and demographic burdens but also at establishing a more decentralized, inclusive, and sustainable of governance [1]. However, this monumental transition also poses significant challenges in the realm of national defense and security. The geographical proximity of IKN to border regions, combined with its design as a high-tech smart city, makes it vulnerable to a wide spectrum of contemporary threats [2]. These threats encompass both conventional and non-conventional dimensions, including cyberattacks, ecological disasters, and potential social disruptions that may undermine national stability. Within this context, the development of an intelligent defense architecture focused on system integration and multidimensional resilience becomes imperative to ensure public security and long-term preparedness for the new capital [3]. This approach aligns with the focus of the International Journal of Safety and Security Engineering, which emphasizes the importance of integrating technology, security system engineering, and smart city design to achieve adaptive public safety in response to complex threats arising from technology and environmental factors.

While discussions on the development of Indonesia's IKN have largely emphasized spatial, ecological, and digital transformation, the systematic design of defense and public security systems has received limited attention, resulting in the absence of a conceptual framework that integrates military, cyber, environmental, and social dimensions. This gap poses potential risks to national resilience, as IKN may become vulnerable without an adaptive and integrated defense strategy informed by institutional, infrastructural, and socio-technological threat assessments. Addressing this challenge, the present study proposes an intelligent defense architecture model for the IKN that integrates inter-agency coordination, cybersecurity, and technology-based risk management, aligning with sustainable smart city principles and safety and security engineering frameworks. By emphasizing data

interoperability, predictive analytics, and adaptive decision-making, this research seeks to establish a technology-driven and integrated defense system architecture and to identify the key components required for managing multidimensional public security challenges in the new capital.

The primary contribution of this study lies in the development of a conceptual and implementable framework for technology-based national defense, which can serve as a reference for formulating public security policies in national strategic areas. The proposed model integrates the total defense approach, institutional coordination, and digital defense technologies such as smart surveillance, early warning systems, and adaptive command structures [4]. This approach reflects the principles of integrated security design as advanced in the field of safety and security engineering, wherein the interconnection between technology, policy, and societal preparedness forms the cornerstone of long-term resilience for strategic urban environments.

The structure of this article is organized into five sections. Section 1 outlines the background, research problems, objectives, and contributions of the study. Section 2 reviews the related literature. Section 3 presents the research methodology, which employs an exploratory qualitative approach combined with Strengths, Weaknesses, Opportunities, and Threats (SWOT) and Analytic Hierarchy Process (AHP) analyses. Section 4 discusses the key findings related to the design of the intelligent defense architecture, threat mapping, and the evaluation of infrastructure and human resources (HR) readiness. Section 5 presents the conclusions and policy implications.

The urgency of this research lies in the necessity to establish a national defense architecture that is intelligent, integrated, and sustainable to address the growing complexity of future threats within the strategic context of Indonesia's new capital city. Without a robust and collaborative security foundation, the IKN project risks systemic vulnerabilities that could jeopardize national stability. Therefore, this study is expected to make a significant contribution to the development of a public security and national defense paradigm grounded in intelligent technologies, aligned with Indonesia's vision of resilience in the 21st century. Consequently, this research not only holds strategic value for national policy formulation but also provides substantial academic contributions to the advancement of theory and practice in safety and security engineering at the global level, particularly in the context of designing smart and secure cities.

Despite the growing body of literature on smart city security and defense system modernization, most existing studies address technological security, governance, and national resilience as separate analytical domains. Integrated defense architecture designs that systematically combine these dimensions within a structured decision-support framework remain limited, particularly in the context of newly established capital cities. In Indonesia's IKN, current discussions and planning efforts largely emphasize infrastructure development and administrative relocation, while prioritized and methodologically transparent defense architecture design receives comparatively less attention. This gap underscores the need for an integrative approach that links strategic security factors with actionable defense priorities tailored to IKN's multidimensional threat environment.

Accordingly, this study is scoped as a conceptual and policy-analytic investigation rather than an empirical or experimental assessment. It relies on secondary data drawn from national defense policies, strategic planning documents, and international capital city security cases, and applies a structured decision-support approach that combines SWOT analysis and the AHP. The study aims to develop an integrated smart defense architecture for IKN, to prioritize key defense components based on their strategic relevance, and to provide policy-relevant insights that support defense governance, inter-agency coordination, and phased implementation planning. This paper does not conduct operational testing or system deployment, but instead offers a structured framework to inform adaptive, technology-driven, and sustainable defense planning for emerging capital cities.

2. LITERATURE REVIEW

Research on security systems for urban and strategic environments has increasingly emphasized smart city security, particularly the integration of digital technologies such as sensors, data analytics, and intelligent surveillance to enhance urban safety and governance efficiency. Existing studies highlight the role of technology-enabled security in addressing civilian threats, cyber risks, and emergency response within urban systems. However, these frameworks often prioritize service optimization and urban management, while defense-oriented considerations and national resilience remain secondary or implicitly addressed, limiting their applicability to strategically sensitive capital cities [5].

A second stream of literature focuses on defense-in-depth and layered defense systems, which originate from military strategy and critical infrastructure protection studies. This body of work underscores the importance of multiple, mutually reinforcing security layers to enhance resilience against complex and evolving threats. While defense-in-depth provides a robust conceptual foundation for risk mitigation and system survivability, prior studies tend to emphasize physical and military dimensions, with less attention to the integration of smart technologies, digital governance, and cross-sector coordination required in modern capital cities [6].

Another prominent stream examines Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) governance, emphasizing the central role of integrated command, control, communications, intelligence, surveillance, and reconnaissance systems in improving situational awareness and coordinated decision-making. Previous research identifies C4ISR as a critical enabler of effective security operations across military, governmental, and civilian institutions. Nevertheless, much of this literature treats C4ISR as a standalone capability, rather than embedding it within a prioritized and holistic defense architecture that balances technological capacity with governance and resilience considerations in a smart city context [7].

The application of multi-criteria decision-making methods, particularly the AHP, represents another relevant stream within security and defense studies. Prior research demonstrates that AHP is effective in structuring complex security decisions and prioritizing alternatives based on systematic judgment. However, existing applications often focus on isolated security sectors or specific infrastructure assets, and rarely integrate AHP with strategic situational analysis tools such as SWOT to bridge qualitative threat assessment with quantitative prioritization at the capital city level [8].

Finally, studies on resilient governance emphasize the importance of institutional adaptability, inter-agency collaboration, and policy coherence in responding to multidimensional security challenges. This literature highlights governance capacity as a key determinant of long-term security effectiveness in complex urban systems. Despite its relevance, resilient governance research is frequently disconnected from concrete defense architecture design and lacks integration with structured decision-support methodologies and technological security frameworks.

In contrast to these existing streams, this study positions itself at the intersection of smart city security, defense-in-depth, C4ISR governance, decision-support methodologies, and resilient governance. By integrating SWOT analysis with the AHP, the proposed framework systematically links qualitative strategic assessments to quantitatively prioritized defense components within a unified smart defense architecture tailored to Indonesia's IKN. This integrative positioning distinguishes the present study from prior research by offering a structured, policy-relevant approach that aligns technological capabilities, governance mechanisms, and national resilience considerations within a single decision-support framework.

3. METHOD

This study employs an exploratory-descriptive qualitative approach with an applied case study design, aimed at developing an intelligent defense architecture for IKN as a prototype of a smart city and Indonesia's new administrative center. This approach was selected for its ability to explore in depth the dynamics and complexity of modern defense systems that integrate physical, cyber, social, and environmental security dimensions. The exploratory approach is utilized to investigate conceptual potentials and global practices related to the design of adaptive, technology-based defense systems, while the descriptive approach systematically maps the interrelations between urban infrastructure, public security, and institutional readiness at the national level. The case study design was chosen to enable a comprehensive analysis of IKN's unique context geographically, geopolitically, and in terms of its governance structure as a representative model for new capital city development in the digital era. Within the framework of safety and security engineering, this methodological design also serves to identify the interconnections between defense systems engineering, risk analysis, and preparedness mechanisms against Hybrid and Multidomain Threats that may impact the operational stability of IKN as a smart city.

This study is designed as a conceptual and policy-analytic evaluation rather than an experimental investigation. It adopts a decision-structuring approach to support strategic defense planning for Indonesia's IKN. The inputs of the study consist of authoritative policy documents, national defense regulations, strategic planning reports, and comparative case studies of security systems implemented in international capital cities. These inputs are analytically transformed through a structured methodological sequence, beginning with a SWOT analysis to identify key internal and external security factors, followed by the formulation of strategic criteria, and subsequently prioritized using the AHP. The outputs of this study include a ranked set of defense priorities and an integrated smart defense architecture framework, which together provide a systematic decision-support tool for policy formulation, governance coordination, and adaptive security planning in the context of a newly established capital city.

The object of this research is the national defense system integrated within the smart city architecture of IKN, focusing on several key domains: conventional defense, cybersecurity, technological intelligence, environmental security, and social resilience. The research setting is conceptual, centered on East Kalimantan as the designated region for IKN, while the data used are secondary, obtained through documentary analysis of official documents, strategic reports, and international scholarly publications. A non-participatory, documentation-based approach was employed, as this study does not involve human subjects or direct interviews but rather examines data derived from policy sources and credible literature [9]. This approach enables a structured analysis of the interconnection between public security policies and defense technology systems, which are essential elements in implementing the principles of the safety management system and risk-based defense design.

The primary data sources include legal and national policy documents such as Law No. 3 of 2022 on the State Capital (IKN), the National Long-Term Development Plan (RPJPN) 2025-2045, the Indonesian National Armed Forces (TNI) defense strategy, and the cybersecurity policies of the National Cyber and Encryption Agency (BSSN). In addition, international academic literature and white papers are utilized to strengthen the conceptual foundation, encompassing references on Artificial Intelligence (AI), the Internet of Things (IoT), C4ISR, and smart surveillance systems as key elements in the integration of digital and physical security. Comparative case studies of new capital cities around the world, such as Canberra (Australia), Brasília (Brazil), and Astana (Kazakhstan), are also analyzed to identify best practices in modern urban defense design and multidomain security strategies. This comparative analysis further aims to identify the application of security engineering principles in urban governance, including the design of critical infrastructure, the integration of early warning systems, and adaptive risk control mechanisms responsive to evolving global threats.

Data analysis in this study was conducted through two methodological stages. First, a SWOT analysis was employed to identify internal and external factors influencing the defense readiness of IKN [10]. This analysis encompasses policy, institutional, technological infrastructure, as well as social and geographical dimensions that affect urban security. Second, the AHP was applied to determine strategic priorities among the various components of the defense system [11]. This approach involved pairwise comparisons of key elements such as the effectiveness of command and control systems, digital infrastructure security, inter-agency collaboration, and the adoption of intelligent technologies. The AHP results produced a strategic priority map that serves as a foundation for formulating measurable, integrated, and adaptive defense policies and planning for IKN in response to evolving risks. The combined use of the SWOT-AHP methodology aligns with approaches in safety and security engineering, which emphasize quantitative risk analysis and evidence-based prioritization to support the design of resilient and efficient intelligent defense systems.

Although this study is based on secondary and document-based data, the AHP requires explicit judgment inputs to perform pairwise comparisons. Accordingly, the pairwise

comparison matrices were constructed by the research team through a structured synthesis of authoritative secondary sources, including national defense policy documents, strategic security regulations, official government reports, and comparative case studies of security systems in international capital cities. These sources were systematically reviewed to extract relative importance statements and strategic priorities, which were then translated into AHP judgments using the standard Saaty fundamental scale [12], where a value of 1 represents equal importance, and 9 indicates extreme importance of one criterion over another. The pairwise comparisons were conducted independently by three raters with academic and professional backgrounds in security studies and defense policy, and the resulting individual judgment matrices were aggregated using the geometric mean method to ensure balanced representation. To ensure the logical consistency and reliability of the results, the Consistency Ratio (CR) was calculated for each comparison matrix, and all matrices satisfied the acceptable threshold of $CR \leq 0.10$, indicating that the judgments were sufficiently consistent and that the resulting priority weights are reliable, transparent, and reproducible for decision-support analysis in policy-oriented security research.

To ensure data validity and reliability, source triangulation was conducted by comparing findings from government documents, academic publications, and international case studies. In addition, a focused literature review was employed to ensure logical consistency between the analytical results, theoretical framework, and the context of IKN's development as a sustainable smart city. Theoretical validation was further carried out by examining the conformity of the analysis results with the principles of the Total Defense Theory [13] and the Integrated Defense System Concept [14], both of which emphasize the importance of institutional integration, cross-sectoral coordination, and the application of digital technologies in establishing an effective defense system. This validation process also refers to the safety validation framework commonly applied in technosystem security research, ensuring that the proposed intelligent defense architecture for IKN meets the standards of interoperability, system redundancy, and functional reliability that define modern security engineering.

This methodological approach enables the study to produce an adaptive, technology-driven defense architecture model oriented toward public security, in alignment with national security objectives and sustainability principles. Consequently, this research not only contributes theoretically to the advancement of the smart defense architecture concept within modern security studies but also provides a practical framework for the planning and implementation of future defense policies for IKN. Moreover, the methodological outcomes are expected to contribute to the broader development of safety and security engineering, particularly in the application of integrated digital physical defense systems for the protection of critical infrastructure and the enhancement of public safety within high-technology smart city environments.

4. RESULTS AND DISCUSSION

The result of this study indicates that the development of the defense system for IKN requires an integrative approach that unites technological, institutional, and social dimensions within a single adaptive national security architecture. Through the implementation of the smart defense concept, IKN is envisioned as an intelligent defense hub that combines military and non-military strengths through a unified C4ISR-based command system, the use of AI for surveillance, and multi-layered protection of digital infrastructure. This integration creates synergy among physical, cyber, and social defense components, allowing each element not only to function independently but also to reinforce one another in detecting, analyzing, and responding to threats in real-time. With this approach, the IKN defense system is designed not merely for protective purposes but also to develop predictive and collaborative capabilities that strengthen national resilience in a sustainable manner amid the evolving dynamics of modern threats.

4.1 Intelligent defense architecture of Nusantara Capital City: The integrative foundation of the national security system

The development of IKN as Indonesia's new administrative center presents strategic and multidimensional challenges in designing a comprehensive defense system. The relocation of the national capital from Jakarta to Nusantara is not merely an administrative shift but a transformation of paradigm in safeguarding national sovereignty and security. As the political, economic, and governmental center of gravity, IKN must possess a defense system that is not only militarily robust but also adaptive to the evolving landscape of contemporary threats, both physical and cyber. This approach aligns with the principles of safety and security engineering, which demand the integration of defense, public security, and information technology within a unified command system resilient to multidomain disruptions. In the context of security systems engineering, IKN serves as a strategic laboratory for the implementation of defense mechanisms driven by AI and predictive analytics to detect, prevent, and respond to threats in real-time.

The defense architecture of the Capital City of Nusantara is designed to integrate conventional defense approaches with cutting-edge technologies such as AI, big data-driven surveillance systems, and coordinated communication and control networks. Its legal framework is founded on Law No. 3 of 2022 on the State Capital, Presidential Regulation No. 63 of 2022 on the Master Plan of IKN, and the Minister of Defense Decree No. KEP/1746/M/XII/2023 on the Master Plan for the Development of the National Defense System in IKN Nusantara [15]. Within the context of modern security engineering, the combination of regulatory structure, digital infrastructure, and multidimensional defense strategies forms a crucial pillar in realizing a security system characterized by redundancy, interoperability, and responsiveness to systemic threats in the digital era.

Within this framework, the defense system of the Capital City of Nusantara adopts the Total Defense concept, which entails the participation of all citizens, all regions, and all national resources in safeguarding the sovereignty of the state. Accordingly, IKN functions as the nation's strategic center of gravity, protected through the comprehensive mobilization of national potential not only through military power but also by integrating the strength of the people, natural resources, and national infrastructure [16]. This total defense approach is combined with the principles of safety governance, whereby all security subsystems, physical, digital, and social, are

organized within a unified command architecture to ensure the capital city's resilience and functional sustainability.

The defense system architecture of the Capital City of Nusantara is built upon four interrelated core components that collectively establish a multilayered security framework. The intelligence component functions in early detection, threat analysis, and the provision of strategic information through an integrated surveillance system supported by predictive analytics. The defense component coordinates both military and non-military forces under a territorial-based defensive deterrence strategy, ensuring synergy among the Indonesian National Armed Forces (TNI), the National Police (Polri), and national reserve components [17]. The security component is responsible for maintaining public order, enforcing the law, and protecting critical infrastructure. Meanwhile, the cyber component safeguards IKN's strategic information systems and digital infrastructure from potential cyberattacks. Together, these four components constitute a layered defense system consistent with international security engineering standards, wherein each layer is designed to reinforce the others through fail-safe and early-warning mechanisms to ensure the city's operational continuity and the safety of its inhabitants.

The smart defense concept of the IKN serves as the integrative framework for these four components, combining hard defense (military defense) and soft defense (non-military defense), complemented by elements of security diplomacy within a dual strategy system approach. The three core elements of smart defense, sensor, shooter, and command control, are operated synergistically within a multi-domain integration system. This smart defense approach reflects the principles of modern security systems engineering, in which sensory networks, predictive algorithms, and autonomous control systems operate cohesively to enhance situational awareness and accelerate response capabilities against emerging threats. The implementation of this system also emphasizes principles of sustainability, public safety, and energy efficiency, ensuring that defense innovation aligns with the broader goals of sustainable and secure urban governance.

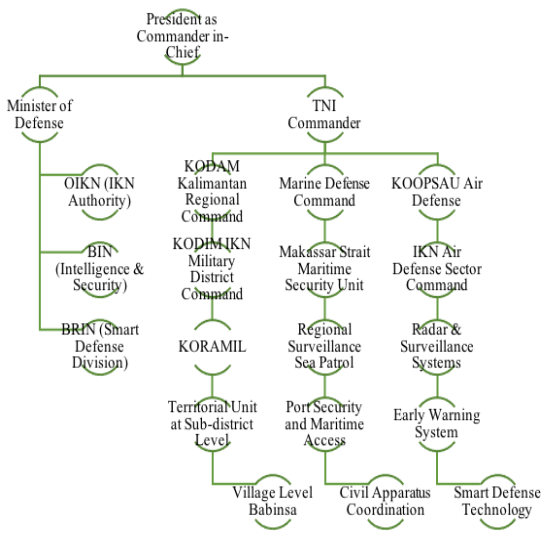

Figure 1. Strategic-tactical command structure of the Nusantara Capital City (IKN) defense system

The Anti-Access/Area Denial (A2/AD) strategy is also adopted within the context of the IKN to prevent adversaries from gaining access to the capital's strategic areas. Through the deployment of defense assets across land, sea, and air domains, this system leverages precision radar technology, resilient communication networks, and predictive AI systems. The A2/AD approach is further reinforced by the synergy among the Coordinating Ministry for Political, Legal, and Security Affairs, the Ministry of Defense, the Indonesian National Armed Forces (TNI), the Nusantara Capital Authority (OIKN), the National Research and Innovation Agency (BRIN), and the National Police (Polri) in adapting advancements in modern defense technology, including the use of unmanned aerial vehicles (UAVs) and military robotic systems. From a safety and security engineering perspective, the implementation of the A2/AD strategy in IKN is not limited to deterring military threats but also extends to protecting critical infrastructure and maintaining the functionality of public communication networks during crises. This represents the application of resilient infrastructure design principles within a technology-based national defense framework. The analytical framework used in this study is illustrated in Figure 1.

The defense command structure of IKN is organized within an integrated hierarchy that extends from the strategic to the tactical level. At the strategic level, the highest command authority rests with the President of the Republic of Indonesia as the Supreme Commander of the Armed Forces (as stipulated in Article 17 of the 1945 Constitution), supported by the Minister of Defense as the principal policy formulator and the Commander of the Indonesian National Armed Forces (TNI) as the chief operational executor. Inter-agency coordination involves the Nusantara Capital Authority (OIKN), the State Intelligence Agency (BIN), and the National Research and Innovation Agency (BRIN) in conducting research and development related to the smart defense concept [18]. This cross institutional collaboration exemplifies the application of an integrated safety governance model, which serves as a cornerstone in constructing a science-based national security system. Through the integration of policy, research, and command systems, IKN's defense architecture is designed to effectively adapt to technological advancements and evolving multidomain threats.

At the operational level, joint command is executed by the Regional Military Command (KODAM) of Kalimantan, the Fleet Command (KOARMADA), and the Air Operations Command (KOOPSAU), integrating land, sea, and air operations while maintaining control over strategic areas such as the Makassar Strait [19]. The IKN Air Defense Sector Command has been established under the Indonesian Air Force (TNI AU) and is planned to be relocated to Nusantara. This integration supports the implementation of the system-of-systems engineering concept, wherein air, land, and maritime defense subsystems operate synergistically within a unified information architecture that enables real-time data exchange. Such an arrangement enhances command efficiency and minimizes the risk of system failure due to inter-branch coordination fragmentation.

Meanwhile, at the tactical level, coordination is carried out by District Military Commands (KODIM) and Subdistrict Military Commands (KORAMIL) stationed within IKN, responsible for protecting development projects, conducting patrols, and maintaining security across administrative zones [20]. At this level, the principles of public safety engineering become essential. The deployment of tactical units around construction zones serves not only physical protection purposes but also ensures social stability and the continuity of

public activities throughout the development phase. Thus, the defense system of IKN is designed not only to uphold national sovereignty but also to safeguard the safety and resilience of the community within it.

4.2 Multi-layer defense model: Physical, digital, and social integration for public security

The multi-layer defense architecture of the IKN is based on the defense in-depth principle, employing multiple and mutually reinforcing layers to ensure continuity against hybrid and multidomain threats. Integrated within a unified smart defense architecture, this model combines physical, digital, and social security systems in line with Safety and Security Systems Engineering principles that emphasize redundancy, interoperability, and multidomain integration. By safeguarding critical infrastructure, public spaces, and government facilities through a system-of-systems approach that integrates surveillance, adaptive control, and predictive risk analysis, IKN's security is conceptualized not merely as a militaristic arrangement but as a resilient and intelligent engineering outcome harmonizing human, technological, and infrastructural dimensions.

Physical Layer: Infrastructure and Public Space Defense, the first layer of the defense system in the IKN is the physical layer, which functions as the primary line of defense against direct threats. This system employs perimeter fencing, access control posts, motion sensors, and CCTV surveillance networks. Physical security is further reinforced through routine patrols, automated detectors, and AI-based motion sensor integration, all of which are directly connected to a centralized security control center.

This surveillance infrastructure operates under the principle of layered physical defense, which not only focuses on detection and deterrence but also provides critical response time for defense units to act swiftly. Digital access control technologies enable early detection of security breaches through smart gate systems integrated into the IKN smart defense 5.0 platform [21].

Furthermore, the spatial configuration of physical defense is strategically designed to support the A2/AD strategy, involving the deployment of strategic monitoring points that facilitate rapid response to potential threats targeting vital assets such as government centers, main transportation routes, and national energy zones. This approach applies the principles of protective infrastructure design within the field of security engineering, emphasizing structural resilience and public safety. By integrating intelligent sensors, spatial defense design, and adaptive control systems, IKN's physical defense layer is engineered to maintain a high degree of resilience against physical disruptions and extreme environmental conditions.

Digital Layer: Cybersecurity and Integrated Command, the second layer focuses on cybersecurity and strategic information systems, which serve as the backbone of IKN's operations as a smart city. The digital components include the implementation of firewalls, VPNs, intrusion detection and prevention systems (IDS/IPS), as well as network segmentation (DMZ) and end-to-end data encryption.

An initial study on the cybersecurity framework in IKN emphasizes the importance of digital log audits, centralized access control systems, and cybersecurity training for both operators and citizens as part of an adaptive security strategy [22]. The implementation of smart defense 5.0 further expands the use of drones, advanced radar systems, and virtual maritime technology (VMT) in coastal areas. These technologies support automated, real-time monitoring in the Makassar Strait and strategic airspace, as part of an integrated air and maritime defense control system [23].

This digital layer is directly connected to the integrated command center (fusion center), which functions as a communication hub between cyber systems, radar, and territorial surveillance. This integration endows IKN with a highly resilient cyber-physical system, in line with the characteristics of engineering-based security systems. The approach embodies the principles of cyber-physical integration engineering, where digital and physical security are unified through adaptive algorithms and predictive detection models. It enables automated decision-making processes and efficient coordination of responses to cross-domain threats.

Social Layer: Community Resilience and Civil-Military Collaboration, the third layer emphasizes social resilience as part of the soft defense strategy. This approach positions the community as a "human firewall," a non-technical line of defense that detects and reports social threats while supporting public order.

Community involvement is realized through civil-military coordination forums, security-focused community FGDs, and public awareness campaigns addressing cyber threats and radicalism [24]. Public security education programs enhance societal defense literacy, foster a sense of collective responsibility, and establish two-way communication between citizens, security forces, and defense institutions. Within the framework of safety and resilience engineering, this social layer functions as an adaptive component that strengthens the community's capacity to respond to crises. Through multi-stakeholder collaboration, IKN's social defense system ensures the continuity of public services and reinforces social legitimacy for the national defense system.

This social approach reinforces the principles of soft defense within smart defense, where defense begins with the participation of local communities, in line with the values of inclusivity and democracy that underpin the development of IKN as a smart capital.

Integration of the Three Layers: Command, Visualization, and Response, the three defense layers, physical, digital, and social, are integrated through the Command and Control Room, Fusion Center, and Digital Twin System. The digital twin system functions as a real-time virtual replica of IKN's infrastructure and security activities, providing direct visualization of physical conditions, cyber threats, and social dynamics. AI-driven anomaly detection and data-correlation models are increasingly applied to identify cyber threats in complex and interconnected digital infrastructures [25].

Cross layer integration enables the synchronization of threat detection and operational response, whereby the physical layer provides early warnings, the digital layer verifies and analyzes risks, and the social layer supports information validation and on-ground mitigation. This multi-layered defense model enhances redundancy and adaptability, exemplifying the practical application of Safety and Security Systems Engineering through real-time, cross-domain coordination. As a result, IKN's defense architecture is not only protective but also predictive and collaborative, positioning it as a resilient smart capital security model with potential applicability to other strategic areas.

4.3 Integration of technology, national resilience, and public security in the Nusantara Capital City

The defense architecture of the IKN is designed to address multidimensional security challenges in the modern era through the integration of technology, national defense policies, and strategic risk governance. This integration aims not only to establish a robust and efficient security system but also to ensure national resilience and sustainability against threats that are physical, digital, social, or ecological in nature [26]. This integrative approach aligns with the principles of safety and security engineering, which emphasize the importance of coherence among system components, humans, technology, policies, and infrastructure to achieve sustainable public security. In the context of IKN, this integration also seeks to create a national defense system oriented toward risk prediction, proactive prevention, and adaptive response to multi-domain threats.

IKN's defense system is built by combining advanced technological infrastructure with cross-sector institutional coordination, encompassing the military, police, civil authorities, and national research institutions within a unified smart defense architecture. This approach positions technology as both an enhancer of defense policy effectiveness and a guarantor of public security. The cross-sectoral framework is central to modern security system engineering, as it enables the creation of an interoperable defense framework capable of rapidly and efficiently adapting to evolving threats.

The implementation of the C4ISR serves as the foundational framework for integrating IKN's defense system. C4ISR functions as the primary control hub, connecting all security layers, from physical and cyber defenses to social protection. It encompasses early warning systems, secure communication networks, radar installations, and national defense data centers that provide real-time situational awareness. This system enables adaptive responses to hybrid threatsincluding cyberattacks and social disturbances, through a combination of AI-driven surveillance, big data analytics, and encrypted communication networks. The integration of C4ISR also exemplifies the application of cyber-physical resilience engineering, positioning distributed control systems and predictive analytics as critical elements in ensuring multi-layered security and operational continuity for a smart city defense system such as IKN.

The success of IKN's defense system heavily relies on the readiness of infrastructure and the competencies of HR capable of operating advanced technologies. A study by Sensuse et al. [22] identified gaps between technological requirements and the operational capabilities of defense personnel. Therefore, tiered training programs, national certification, and collaboration with defense educational institutions are prioritized to ensure the effective management of AI and data-driven systems. Strengthening HR capacity contributes to the human reliability engineering pillar, wherein humans act as adaptive elements linking AI with strategic decision-making within the national defense system.

Beyond technological factors, the design of IKN's defense architecture also draws lessons from other national capitals. Canberra, for instance, stands out for integrating community-based social defense with public early warning systems [27]; Brasília emphasizes the use of an integrated C4ISR center for real-time military and civil coordination [28]; while Astana (Kazakhstan) demonstrates the importance of integrative planning from the urban design stage, combining technology with social control mechanisms [29]. These insights serve as references for adapting IKN's defense system to Indonesia's geographical and social context, particularly in balancing technological capabilities with community participation. Such comparisons strengthen the methodological relevance of this study through a comparative safety engineering approach, focusing on the transferability of best practices in developing a smart city-based national security system.

Although the integrated defense system for IKN demonstrates a strong conceptual foundation, its implementation faces significant institutional, technological, and infrastructural challenges. Overlapping authorities among the Ministry of Defense, the Indonesian National Police, the State Intelligence Agency, and the IKN Authority may hinder timely decision-making during crises, while limited interoperability among radar, communication, and sensor systems constrains effective inter-agency coordination. These challenges underscore the need for standardized national defense communication protocols as a prerequisite for integrated cyber-physical security systems. Furthermore, infrastructure readiness in IKN's buffer zones remains critical, as East Kalimantan's geographic and logistical conditions require resilient military-civilian transportation networks and real-time logistics monitoring to ensure rapid troop and equipment mobility during natural or ecological emergencies. Together, these measures align with resilient logistics and safety network design principles to support an adaptive and secure defense system under environmental constraints.

Threat mapping for the IKN covers cyber, ecological, and social dimensions within Hybrid and Multidomain Threats. Cyber risks target smart city infrastructure [30], ecological hazards require AI-based early detection, and social threats such as terrorism remain significant due to IKN's strategic location. Although mitigation efforts involve national early warning systems and inter-agency training, data integration remains limited. Prior research notes that AI-enabled command systems face governance and interoperability challenges [31]. Consequently, the lack of integrated monitoring and intelligence systems may hinder effective response, emphasizing the need for a unified risk management framework.

Table 1. Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of the Nusantara Capital City (IKN) defense

Strengths	Weaknesses
Full support from the central government for IKN development and its defense	Defense infrastructure readiness is not yet optimal
Integration of smart city concepts with smart defense	Defense human resources (HR) gaps in advanced technologies
Strategic geographic location, far from regional conflict centers	Inter-agency coordination is not yet solid
Opportunities	**Threats**
Advancements in AI, IoT, and early warning systems	Cyberattack threats to critical infrastructure
Potential for international collaboration and domestic defense industry development	Potential social radicalization in border regions
Strengthening of legal frameworks and new regulations	Ecological, cyber, hybrid, and logistical threats

To comprehensively understand the strategic positioning of

IKN's defense system, a SWOT analysis was conducted to systematically identify and evaluate its key SWOT. This analytical approach enables a structured assessment of both internal and external factors influencing the effectiveness, resilience, and sustainability of the proposed defense architecture. By examining institutional capacity, technological readiness, regulatory support, and emerging security risks, the SWOT analysis provides an integrated strategic overview that supports evidence-based decision-making. The results of this analysis serve as the foundation for subsequent prioritization and system design processes and are summarized in the following Table 1.

The analysis shows that IKN's defense system benefits from strong political support and national regulatory backing, alongside opportunities driven by technological advancement and international collaboration, while persistent weaknesses in infrastructure readiness and HR capacity remain significant constraints amid external cyber and social radicalization threats. Accordingly, IKN's security development strategy should prioritize deeper integration between technology and institutional structures to enable timely and calibrated responses, coupled with strengthened HR development and supportive regulatory frameworks. This integrated approach positions IKN's defense architecture not merely as a physical protection mechanism but as a strategic instrument for building sustainable and resilient national security, consistent with the principles of Safety and Security Systems Engineering and offering a replicable model for smart capital defense in the digital era. The classification of SWOT factors into AHP criteria is shown in Table 2.

Table 2. Mapping of SWOT factors to AHP criteria

Strengths	Weaknesses
Existing national defense command structure (supports C4ISR as an integrated command and control system)	Fragmented inter-agency coordination (weakens inter-agency collaboration effectiveness)
Government commitment to digital transformation (enables AI-based surveillance adoption)	Limited cybersecurity readiness (affects digital infrastructure security)
Institutional support for smart defense development (reinforces C4ISR governance capacity)	Gaps in technical capacity for advanced digital security (increase cyber vulnerability)
Opportunities	**Threats**
Advancement of AI and smart city technologies (strengthen AI-based surveillance capabilities)	Cyber-attacks and hybrid warfare risks (challenge digital infrastructure security resilience)
International security cooperation (enhances inter-agency collaboration mechanisms)	Multidimensional and asymmetric threats (require integrated C4ISR situational awareness)
Expansion of digital governance and security regulations (support C4ISR-based coordination)	Increasing complexity of cyber and information warfare (pressure on integrated command systems)

Note: SWOT = Strengths, Weaknesses, Opportunities, and Threats; AHP = Analytic Hierarchy Process; C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance; AI = Artificial Intelligence.

To ensure a structured and non-ad hoc prioritization process, the SWOT analysis results were systematically mapped onto the AHP criteria. Internal factors (Strengths and Weaknesses) were linked to system capability, technological readiness, and institutional coordination, while external factors (Opportunities and Threats) were associated with environmental uncertainty and adaptive command and control needs. Based on this mapping, the SWOT findings were translated into four AHP criteria: C4ISR capability, AI-based surveillance, digital infrastructure security, and inter-agency collaboration, ensuring that the pairwise comparisons and priority weights were derived from coherent strategic reasoning rather than subjective judgment.

4.4 Integrated defense system design and strategic priority analysis of the Nusantara Capital City

The integrated defense system of the IKN embodies Indonesia's Total Defence principles by combining military, civil, and community components within a layered and interoperable national security architecture. Grounded in safety and security systems engineering, this design emphasizes cross-sector collaboration, adaptive resilience, and system interoperability to ensure the continuity of governance and public security. While the military addresses external and strategic threats, civil institutions such as the Indonesian National Police, the National Counter-Terrorism Agency, and regional governments manage domestic security and socio-ecological risks, supported by community participation as a non-military defense element (Sishankamrata) functioning as human sensors in early warning systems. This smart total defense approach reinforces national security as a shared responsibility and strengthens community resilience as a core pillar of modern defense architecture.

The effectiveness of IKN's defense system depends on the integration of modern defense technologies centered on C4ISR, which serves as a real-time command hub connecting military, civil, and community units. Supported by coordinated smart CCTV, environmental sensors, defense radar, reconnaissance drones, and AI-based early warning systems, the C4ISR framework is designed in line with cyber-physical security principles to ensure secure and continuous operations during crises. In parallel, the defense architecture incorporates evacuation and emergency response planning for natural disasters and security threats, with routes and safe zones communicated through smart applications, digital information boards, and routine drills, highlighting that IKN's smart defense approach emphasizes preparedness and impact mitigation as an adaptive civil protection mechanism against multidimensional risks in a smart urban environment. Such integrated sensor-based monitoring and real-time alert systems are consistent with safety and security systems engineering approaches applied in smart and critical environments [32].

To determine development priorities for components within IKN's defense system, the AHP method is employed, allowing policymakers to evaluate strategic elements in a measurable and objective manner. Four key elements are assessed: (1) Command and Control System (C4ISR), (2) AI-based Surveillance, (3) Digital Infrastructure Security, and (4) Inter-agency Collaboration.

The AHP process is conducted through the construction of pairwise comparison matrices, where each element is compared pairwise to determine its relative importance for national defense effectiveness. The evaluation applies the fundamental 1–9 priority scale, where 1 indicates equal importance and 9 represents extreme importance of one

element over another.

This structured approach not only provides a rational and transparent foundation for decision-making but also allows for a comprehensive understanding of the interrelationships among key defense components. Through AHP, policymakers can quantitatively identify which aspects demand greater focus and resource allocation to strengthen IKN's defense posture. Furthermore, the method ensures that strategic decisions are supported by consistent, data-driven analyses rather than subjective judgment alone. In the context of national defense development, the use of AHP therefore plays a critical role in shaping a resilient, adaptive, and well-coordinated defense strategy for IKN.

Table 3. AHP table: Pairwise comparison

Criteria	C4ISR	AI-Based Surveillance	Digital Infrastructure Security	Inter-Agency Collaboration	Row Total
Command and control system	1.00	2.00	3.00	4.00	10.00
AI-based surveillance	0.50	1.00	2.00	3.00	6.50
Digital infrastructure security	0.33	0.50	1.00	2.00	3.83
Inter-agency collaboration	0.25	0.33	0.50	1.00	2.08

Note: AHP = Analytic Hierarchy Process; C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance; AI = Artificial Intelligence.

Table 4. AHP table: Matrix normalization

Criteria	C4ISR (2.08)	AI (3.83)	Digital (6.50)	Collaboration (10.00)	Average (Priority)
Command and control system	0.481	0.522	0.462	0.400	0.466 (46.6%)
AI-based surveillance	0.240	0.261	0.308	0.300	0.277 (27.7%)
Digital infrastructure security	0.158	0.130	0.154	0.200	0.161 (16.1%)
Inter-agency collaboration	0.120	0.086	0.077	0.100	0.096 (9.6%)

Note: AHP = Analytic Hierarchy Process; C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance; AI = Artificial Intelligence.

Based on the pairwise comparison presented in Table 3, the C4ISR component obtained the highest total score of 10.00, indicating that this aspect is considered the most critical for ensuring the effectiveness and success of the national defense system in the IKN. In contrast, inter-agency collaboration received the lowest score of 2.08, suggesting that while cross-agency coordination remains necessary, its contribution is more supportive in relation to the primary strategic elements.

The normalization of the AHP matrix, as shown in Table 4, indicates that C4ISR holds the highest priority weight at 46.6%, followed by AI-based surveillance (27.7%), digital infrastructure security (16.1%), and inter-agency collaboration (9.6%). The total priority weights sum precisely to 1.000 (100%), thereby ensuring methodological consistency and full adherence to standard AHP normalization procedures. These results demonstrate that integrated command and control capability constitutes the backbone of IKN's smart defense architecture, while AI-enabled surveillance and digital infrastructure protection function as critical supporting components. These findings align with the characteristics of systems engineering for safety and security, where defense effectiveness depends on the adaptive, real-time integration of information and communication systems across multiple domains.

The recalculated AHP results indicate that the C4ISR remains the highest-priority component with a weight of 0.466 (46.6%), followed by AI-Based Surveillance at 0.277 (27.7%), Digital Infrastructure Security at 0.161 (16.1%), and Inter-Agency Collaboration at 0.096 (9.6%). The dominance of C4ISR highlights the strategic necessity of establishing an integrated command, control, communication, and intelligence network capable of synchronizing military, civil, and technological defense elements in real time. Such integration enhances situational awareness, accelerates information processing, and enables coordinated responses to hybrid and multidomain threats within the smart city environment of the IKN. Although inter-agency collaboration receives the lowest priority weight, it remains a critical enabling factor that ensures institutional alignment, policy coherence, and operational coordination across sectors. Therefore, the AHP findings confirm that technological integration through C4ISR constitutes the structural backbone of a resilient, adaptive, and responsive national defense architecture.

To ensure methodological rigor, the consistency of the pairwise comparisons was evaluated through the calculation of the Consistency Ratio (CR). Based on a maximum eigenvalue (λmax) of 4.031, the Consistency Index (CI) was computed as $(4.031 - 4)/(4 - 1) = 0.010$. Using the Random Index (RI) value of 0.90 for $n = 4$, the resulting CR was 0.011, which is well below the acceptable threshold of 0.10. This confirms that the judgments applied in the pairwise comparison matrix are logically consistent and statistically reliable. Accordingly, the derived priority weights are methodologically valid and can serve as a robust foundation for strategic decision-making in the development of IKN's integrated smart defense system. The final priority rankings are presented in Table 5.

Table 5. Interpretation of AHP

Priority	Criteria	Result (%)
1	Command and control system (C4ISR)	46.6%
2	AI-based surveillance	27.7%
3	Digital infrastructure security	16.1%
4	Inter-agency collaboration	9.6%

Note: AHP = Analytic Hierarchy Process; C4ISR = Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance; AI = Artificial Intelligence.

Figure 2 illustrates the priority weights of IKN's defense components, with C4ISR ranked highest, followed by AI-based surveillance, digital infrastructure security, and inter-agency collaboration. These results provide strategic guidance for policymakers by emphasizing the need to prioritize C4ISR

and AI surveillance as the core elements of digital and operational defense, while progressively strengthening digital security and inter-agency coordination through integrated regulations, improved interoperability, and joint training. Overall, the findings highlight that IKN's defense architecture depends not only on military capability but also on an intelligent defense ecosystem grounded in data integration, advanced technology, and cross-sector coordination to support sustainable national resilience.

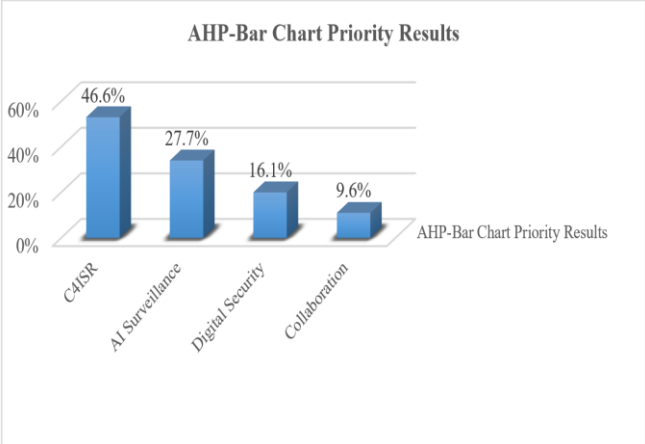

Figure 2. Analytic Hierarchy Process (AHP)-bar chart priority result

The prominence of C4ISR as the highest-priority component in the AHP results reflects IKN's exposure to hybrid and multidomain threats that require real-time situational awareness, rapid information processing, and coordinated decision-making within a smart city environment. As the central integrative backbone of the defense architecture, C4ISR enables the synchronization of intelligence, surveillance, communication, and command across military and civilian domains. Without a robust C4ISR foundation, complementary components such as AI-based surveillance and digital infrastructure security would operate in isolation, thereby reducing the overall effectiveness of the defense system.

In a comparative perspective, the prioritization of C4ISR in IKN is consistent with international capital city experiences such as Canberra, Brasília, and Astana, where integrated command-and-control systems underpin civil-military security coordination. However, IKN places stronger emphasis on digital and AI-enabled coordination to address Indonesia's geographic scale, archipelagic vulnerabilities, and heightened exposure to cyber and hybrid threats. From an implementation standpoint, these findings support a phased development strategy that prioritizes C4ISR infrastructure, followed by the integration of AI-based surveillance and digital security systems, and ultimately the institutionalization of inter-agency collaboration through standardized governance mechanisms, assuming gradual improvements in interoperability and organizational readiness.

Overall, the integrated defense system design of IKN illustrates the synergy between technology, organizational structure, and public participation. This approach combines the principles of layered defense, AI-driven surveillance, and total defense collaboration into a measurable, responsive, and resilient architecture. With the AHP analysis highlighting the superiority of C4ISR as the central command hub, IKN's defense system is expected to serve as a prototype for a technology-based national security model, consistent with the principles of safety and security engineering in the context of a 21st-century smart city. This positions IKN not merely as an administrative capital but as a smart defense laboratory that can serve as a global reference for the development of integrated, technology-driven urban security systems and national resilience.

5. CONCLUSIONS

This study has developed a smart defense architecture model for the IKN, integrating technological, institutional, and societal components within a unified safety and security systems engineering framework. Based on the recalculated AHP normalization procedure, the analysis confirms that the C4ISR constitutes the highest strategic priority with a weight of 0.466 (46.6%), followed by AI-based surveillance at 0.277 (27.7%), digital infrastructure security at 0.161 (16.1%), and inter-agency collaboration at 0.096 (9.6%). The total priority weights sum precisely to 1.000 (100%), ensuring full methodological consistency with standard AHP requirements. Collectively, these four components form the structural foundation of an adaptive and integrated defense system capable of addressing hybrid, cyber, and ecological threats within a smart city environment. The findings reaffirm that effective defense development extends beyond technological sophistication, requiring coordinated governance mechanisms and active community participation to ensure resilience across physical, digital, and social dimensions.

Despite these contributions, the study has several limitations. First, reliance on secondary data may constrain the completeness and timeliness of the information analyzed. Second, although the AHP results demonstrate a satisfactory level of consistency, the method inherently depends on structured expert judgment, which may introduce a degree of subjectivity in weighting and prioritization. Third, while the framework is highly relevant to the context of IKN, its applicability to other urban environments may be influenced by differences in governance structures, technological readiness, and socio-political conditions.

Future research should incorporate primary data collection, including interviews with defense stakeholders and field-based assessments, to further validate and refine the proposed model. Additionally, dynamic simulation techniques and scenario-based analysis could be employed to evaluate system resilience under evolving multidomain threat conditions. Expanding the framework to incorporate emerging technologies, ecological risk modeling, and cross-sector policy integration would further enhance the robustness and transferability of smart defense architectures in other strategic urban settings.

Overall, this study contributes to the advancement of knowledge in international relations, defense studies, and smart city planning by offering a methodologically validated and strategically prioritized defense framework. By integrating technological innovation, governance coordination, and community resilience into a coherent architecture, the research provides both conceptual insight and practical guidance for developing adaptive, resilient, and sustainable urban defense systems in Indonesia and beyond.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to the Directorate of Research and Community Service (DPPM), Universitas Islam Riau (UIR), for the financial support provided through the Internal Research Grant Scheme of UIR 2025, under contract No.: 1251/KONTRAK/P-K-U/DPPM-UIR/07-2025. This support has been invaluable in enabling the successful completion of this research.

REFERENCES

[1] Syaban, A.S.N., Appiah-Opoku, S. (2023). Building Indonesia's new capital city: An in-depth analysis of prospects and challenges from current capital city of Jakarta to Kalimantan. Urban, Planning and Transport Research, 11(1): 2276415. https://doi.org/10.1080/21650020.2023.2276415

[2] Rizkiano, S., Hadiningrat, K.P.S.S. (2024). Smart security development to realize security and public order in the capital city of Nusantara. JIPOWER: Journal of Intellectual Power, 1(2): 61-75. https://doi.org/10.63786/jipower.v1i2.14

[3] Pambudhi, N.A. (2024). Analysis of the development of Indonesia's new national capital and its impact on the defense budget. Jurnal Kewarganegaraan, 8(1): 70-79. https://doi.org/10.31316/jk.v8i1.5992

[4] Wijanarko, T., Supriyadi, A.A., Saputro, G.E., Harefa, F., Kartiningsih, Y., Mardamsyah, A. (2025). The model of integration of defense policy and public policy to address the threat of hybrid warfare to improve national defense. Lebah, 18(3), 286-295. https://doi.org/10.35335/lebah.v18i3.327

[5] Batty, M., Axhausen, K.W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G., Portugali, Y. (2012). Smart cities of the future. The European Physical Journal Special Topics, 214: 481-518. https://doi.org/10.1140/epjst/e2012-01703-3

[6] Trump, B.D., Poinsatte-Jones, K., Elran, M., Allen, C., Srdjevic, B., Merad, M., Vasovic, D.M., Palma-Oliveira, J.M. (2017). Social resilience and critical infrastructure systems. In Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains, pp. 289-299. https://doi.org/10.1007/978-94-024-1123-2_9

[7] Alberts, D.S., Garstka, J.J., Stein, F.P. (1999). Network Centric Warfare: Developing and Leveraging Information Superiority. Department of Defense Command and Control Research Program (DoD CCRP). https://www.dodccrp.org/files/Alberts_NCW.pdf.

[8] Tran, T.A., Ruppert, T., Eigner, G., Abonyi, J. (2022). Retrofitting-based development of brownfield Industry 4.0 and Industry 5.0 solutions. IEEE Access, 10: 64348-64374. https://doi.org/10.1109/ACCESS.2022.3182491

[9] Rusandi, Rusli, M. (2021). Designing basic/descriptive qualitative research and case studies. Al-Ubudiyah: Jurnal Pendidikan Dan Studi Islam, 2(1): 48-60. https://doi.org/10.55623/au.v2i1.18

[10] Inglott, A.S., Schembri, F., Azzopardi, L.M., Mercieca, M. (2016). Swot analysis. Pharmaceutical Technology, 40(4): 40. https://www.pharmtech.com/view/swot-analysis.

[11] Tavana, M., Soltanifar, M., Santos-Arteaga, F.J. (2023). Analytical hierarchy process: Revolution and evolution. Annals of Operations Research, 326(2): 879-907. https://doi.org/10.1007/s10479-021-04432-2

[12] Saaty, T.L. (1980). The Analytic Hierarchy Process. McGraw-Hill, New York.

[13] Rogulis, D. (2024). Understanding Lithuania's total defence approach in the face of Russian threat through principal-agent theory. Security and Defence Quarterly, 49(1): 58-73. https://doi.org/10.35467/sdq/195805

[14] Cilli, M.V. (2015). Improving defense acquisition outcomes using an integrated systems engineering decision management (ISEDM) approach. Doctoral dissertation. Stevens Institute of Technology. https://doi.org/10.13140/RG.2.1.4868.0560

[15] Humas Kemenko Polhukam RI. (2024). Total defense system prepared to protect IKN. https://polkam.go.id/sistem-pertahanan-semesta-disiapkan-untuk-lindungi-ikn/.

[16] Armanto, A.P. (2024). Sustainable development strategy in the Nusantara Capital City (IKN). https://doi.org/10.13140/RG.2.2.13333.54248

[17] Isabela, M.A.C. (2022). 4 components of the total people's defense and security system. Kompas. https://nasional.kompas.com/read/2022/04/10/01000061/4-komponen-sistem-pertahanan-dan-keamanan-rakyat-semesta.

[18] National Research and Innovation Agency (BRIN). (2024). BRIN studies Indonesia's smart defense concept to strengthen the IKN defense system. BRIN. https://www.brin.go.id/news/117764/perkuat-sistem-pertahanan-ikn-brin-kaji-konsep-smart-defense.

[19] Ramadhan, M.G. (2024). Analysis of the tri-service defense strategy in optimizing security for the Nusantara Capital City (IKN). Jurnal Politik Antar Bangsa Globalisme Dan Intermestik, 1(2): 124-139. https://pabgi.ejournal.unri.ac.id/index.php/PABGI/article/view/98.

[20] Nusantara. Nusantara as a superhub. https://www.ikn.go.id/en/about-ikn.

[21] Putra, H., Winarna, A., Bonifasius, B., Albrecht, M., Ghazalie, G. (2024). Smart defense 5.0 to strengthen the defense of Indonesia's capital city (IKN). Jurnal Pendidikan: Teori, Penelitian, dan Pengembangan, 9(2): 110-115. https://doi.org/10.17977/jptpp.v9i2.25390

[22] Sensuse, D.I., Putro, P.A.W., Rachmawati, R., Sunindyo, W.D. (2022). Initial cybersecurity framework in the new capital city of Indonesia: Factors, objectives, and technology. Information, 13(12): 580. https://doi.org/10.3390/info13120580

[23] Azizan, A., Zahra, S., Sophia, S. (2024). Navigating the maritime: Technology for the defense of the Indonesian national capital city (IKN) in the Makassar Strait. Jurnal Pertahanan: Media Informasi Tentang Kajian Dan Strategi Pertahanan Yang Mengedepankan Identity, Nasionalism Dan Integrity, 10(1): 155-168. https://doi.org/10.33172/jp.v10i1.19420

[24] Tarom, M. (2025). The strategic role of defense education in strengthening Indonesia's national security system. Jurnal Pendidikan Dan Pengembangan Sumber Daya Pertahanan, 2(1): 12-19. https://doi.org/10.63210/jp3.v2i1.138

[25] Atmojo, Y.P., Susila, I.M.D., Hariyanti, E., Hostiadi, D.P., Pradipta, G.A., Ayu, P.D.W. (2025). Network anomaly activity detection model based on feature correlation analysis. International Journal of Safety and Security Engineering, 15(9): 1809-1817.

https://doi.org/10.18280/ijsse.150905
[26] Sarjito, A., Risdhianto, A. (2025). Integrating Jakarta smart city technology with a command and control system to strengthen national defense. Contemporary Public Administration Review (CoPAR), 2(2): 143-169. https://doi.org/10.26593/copar.v2i2.8943.143-169
[27] Quilty, J., Dickins, L., Anderson, P., Martin, B. (1986). Capital defence: Social defence for Canberra. https://www.bmartin.cc/pubs/86cd/86cd.pdf.
[28] Brazil Forecast. (2025). Brazilian C4ISR Industry 2025-2033 Analysis: Trends, Competitor Dynamics, and Growth Opportunities. https://www.datainsightsmarket.com/reports/brazilian-c4isr-industry-17810.
[29] Omirgazy, D. (2025). Kazakhstan's digital revolution: From e-government to AI superpower. Kazakh News. https://astanatimes.com/2025/07/kazakhstans-digital-revolution-from-e-government-to-ai-superpower/.
[30] Apriliasari, A.Y., Priyanto, S. (2024). Nusantara Capital City (IKN) and terrorism threat mitigation: A welfare approach to preventing criminal acts in Indonesia. UNES Law Review, 6(4): 11120-11129. https://doi.org/10.31933/unesrev.v6i4.2023
[31] Abdelmaboud, A., Salih, S., Hashim, A.H.A., Almohamedh, R.M., Tajelsier, H., Motwakel, A. (2025). Are GPT-powered AI systems superior to traditional cybersecurity tools: Applications and challenges. International Journal of Safety and Security Engineering, 15(9): 1885-1900. https://doi.org/10.18280/ijsse.150912
[32] Ibraheem, F.N., Ali, Q., Kareem, J.A. (2025). Design and evaluation of a resilient IoT-based safety monitoring system with real-time alerts for industrial environments. International Journal of Safety and Security Engineering, 15(9): 1775-1787. https://doi.org/10.18280/ijsse.150902