



Artificial Intelligence Resilience Data Readiness and Strategic Innovation in Countering Emerging Multidomain Security Threats

Ferdinand Hasudungan Siagian^{1*}, Nefra Firdaus², Sigit Purwanto³, Bangun Pandapotan Hutajulu⁴

^{1,3,4}Universitas Pertahanan Republik Indonesia

²Politeknik Angkatan Darat (POLTEKAD)

Corresponding Author: Ferdinand Hasudungan Siagian fhgian@gmail.com

ARTICLE INFO

Keywords: Artificial Intelligence, Resilience, Data Readiness, Strategic Innovation, Multidomain Security

Received : 16, May

Revised : 18, July

Accepted: 20, September

©2026 Siagian, Firdaus, Purwanto, Hutajulu: This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

The increasing complexity of multidomain security threats requires adaptive defense strategies through the utilization of artificial intelligence (AI), data readiness, and strategic innovation. This study aims to develop an AI-based defense strategy framework by analyzing the relationship between AI resilience, data readiness, and strategic innovation in addressing emerging security threats. The research employs a Design Science Research (DSR) approach supported by literature review and expert validation involving five experts in artificial intelligence, cybersecurity, and information technology. Data analysis was conducted qualitatively through thematic analysis and framework validation evaluation. The results produce a strategic framework that integrates AI resilience, data governance, and innovation to enhance responses toward multidomain security threats. This study contributes to the development of adaptive and sustainable digital defense strategies.

INTRODUCTION

The rapid advancement of Artificial Intelligence (AI) technology has significantly transformed the paradigm of modern security, particularly in addressing complex, dynamic, and multidomain threats. Contemporary security challenges are no longer limited to conventional physical conflicts but have expanded into cyber, information, economic, critical infrastructure, and digital defense domains. The adoption of AI provides substantial opportunities to enhance threat detection, predictive analysis, and strategic decision-making capabilities; however, it also introduces emerging risks, including model manipulation, data-driven attacks, and technology misuse. Vinuesa et al. (2020) emphasized that AI development has broad implications across various sectors but requires effective governance, oversight, and security mechanisms to ensure trustworthy and sustainable implementation.

In the context of digital defense, data readiness has become a fundamental factor because the effectiveness of AI-based systems heavily depends on the quality, security, and availability of data throughout the operational lifecycle. AI systems that lack proper data governance may generate inaccurate decisions and increase vulnerabilities to data-related attacks. Hu et al. (2021) highlighted that AI systems face various security vulnerabilities throughout their lifecycle, including data acquisition, model training, and deployment stages. Therefore, AI resilience has become an essential concept to ensure that AI systems can adapt, maintain functionality, and recover from disruptions or attacks within an increasingly complex security environment.

Globally, various organizations have begun developing strategic approaches to ensure secure and responsible AI adoption. The National Institute of Standards and Technology (NIST), through the Artificial Intelligence Risk Management Framework, emphasizes the importance of managing AI risks through governance, measurement, management, and continuous risk assessment throughout the AI lifecycle (Tabassi, 2023). Furthermore, Dwivedi et al. (2023) explained that the emergence of generative AI expands technological opportunities while simultaneously creating new challenges related to security, information reliability, and technology governance. These developments indicate that future defense strategies require the integration of AI capabilities, data readiness, and strategic innovation to effectively address multidomain security threats in an adaptive manner.

Although research on AI applications in security has grown rapidly, a significant research gap remains regarding the integration of AI resilience, data readiness, and strategic innovation within a comprehensive multidomain defense framework. Previous studies have predominantly focused on the technical application of AI for cyber threat detection, while limited attention has been given to how organizations can establish strategic resilience through the combination of technology, data governance, and continuous innovation. Alshaikh (2021) emphasized the importance of strategic approaches in developing cybersecurity resilience, while Nguyen et al. (2022) demonstrated that AI security challenges require holistic approaches involving both technological capabilities and risk management strategies. This gap highlights

the necessity of developing a framework that integrates technological and strategic defense perspectives.

Based on these challenges, this study aims to develop an Artificial Intelligence-based defense strategy framework by analyzing the relationship between AI resilience, data readiness, and strategic innovation in addressing emerging multidomain security threats. This research applies a Design Science Research (DSR) approach supported by literature analysis and expert validation to develop a strategic framework relevant to modern security requirements. The theoretical contribution of this study is to enrich knowledge regarding the integration of AI resilience, data readiness, and strategic innovation within the field of digital security. Practically, this research provides a foundation for defense organizations, government institutions, and industrial sectors in designing more adaptive and sustainable AI utilization strategies.

The proposed framework is expected to provide a new perspective on how AI can be utilized not only as a technical tool for threat detection but also as a strategic component in building resilient defense systems. This approach extends previous research perspectives that primarily view AI from a technological standpoint by incorporating broader considerations involving technology, human factors, data management, and strategic decision-making. Goh and Vinuesa (2021) stated that effective AI implementation requires appropriate regulation and risk management to maximize technological benefits while minimizing emerging vulnerabilities. Therefore, this study contributes to the advancement of digital security research by proposing an AI-driven defense approach characterized by resilience, data readiness, and strategic innovation.

LITERATURE REVIEW

Artificial Intelligence in the Transformation of Modern Defense Strategies

Artificial Intelligence (AI) has become a strategic technology that significantly transforms modern defense and security paradigms, particularly in addressing increasingly complex, dynamic, and multidomain threats. The capability of AI to process massive volumes of data, identify threat patterns, conduct predictive analysis, and support strategic decision-making has positioned it as a critical component of next-generation defense systems. Unlike conventional security approaches that are primarily reactive, AI enables proactive defense mechanisms through early threat detection, automated response, and continuous learning capabilities. However, the implementation of AI in defense systems requires comprehensive consideration of technological capability, governance, ethical aspects, and operational risks to ensure trustworthy deployment. Sarker (2022) emphasized that AI-based systems provide significant advantages in improving security effectiveness through intelligent automation and predictive analytics, but their success depends on organizational readiness, appropriate risk management, and the integration of technological and human capabilities. Therefore, AI in modern defense should not only be viewed as a computational tool but as a strategic ecosystem involving technology, data, governance, and adaptive decision-making capabilities.

Artificial Intelligence Resilience as a Foundation for Secure and Adaptive Systems

Artificial Intelligence resilience refers to the capability of AI-based systems to maintain functionality, adapt to changing environments, and recover from disruptions, failures, or adversarial attacks. In the context of emerging security threats, AI resilience has become increasingly important because adversaries can exploit vulnerabilities within AI systems through techniques such as adversarial attacks, data poisoning, and model manipulation. A resilient AI system must be able to preserve reliability and accuracy despite hostile conditions throughout its operational lifecycle, including data collection, model training, deployment, and continuous monitoring. Huang et al. (2022) explained that AI security requires a comprehensive approach covering the entire AI lifecycle because vulnerabilities may occur at different stages of system development and implementation. Furthermore, resilience in AI-based defense systems requires mechanisms that support robustness, transparency, adaptability, and continuous improvement. Therefore, AI resilience represents a fundamental capability for developing defense architectures capable of responding effectively to unpredictable and evolving multidomain security challenges.

Data Readiness as a Critical Enabler of Artificial Intelligence Implementation

Data readiness is a fundamental factor determining the effectiveness and reliability of AI-based defense systems because AI performance is highly dependent on the quality, availability, security, and governance of the data used during learning and decision-making processes. In security environments, inaccurate, incomplete, or vulnerable data can significantly reduce AI reliability and potentially create strategic risks. Data readiness includes several dimensions, such as data quality management, interoperability, accessibility, privacy protection, and organizational capability to transform raw information into actionable intelligence. Mikalef et al. (2021) highlighted that organizational AI capability is strongly influenced by the ability to manage digital resources, particularly data-related capabilities that support innovation and decision-making performance. Similarly, recent studies emphasize that AI systems require standardized approaches for evaluating data readiness because poor-quality datasets may lead to inaccurate predictions and unsafe AI outcomes (Hiniduma et al., 2024). Therefore, data readiness should be considered a strategic foundation that enables AI systems to operate effectively, securely, and sustainably in complex defense environments.

Strategic Innovation in Strengthening AI-Based Defense Capabilities

Strategic innovation represents an organization's ability to develop new approaches, processes, and capabilities to respond effectively to changing strategic environments. In the defense sector, innovation is increasingly important because emerging threats evolve faster than traditional security mechanisms. The integration of AI, advanced analytics, and automation provides opportunities to develop more adaptive, predictive, and intelligent defense systems. However, technological adoption alone is insufficient without strategic transformation involving governance, organizational adaptation, and

continuous capability development. Dwivedi et al. (2023) stated that the emergence of advanced AI technologies, particularly generative AI, creates significant opportunities while simultaneously introducing challenges related to security, reliability, governance, and responsible implementation. Consequently, strategic innovation in AI-based defense requires balancing technological advancement with risk management frameworks to ensure sustainable and secure adoption. This perspective demonstrates that innovation should not only focus on acquiring advanced technologies but also on developing organizational capabilities to utilize AI effectively in responding to multidomain security threats.

Multidomain Security Threats and the Need for Integrated AI Defense Frameworks

Emerging multidomain security threats represent a new generation of challenges that simultaneously affect cyber, information, economic, military, and critical infrastructure domains. The interconnected nature of these threats has reduced the effectiveness of traditional defense approaches that operate independently within specific domains. Modern security environments require integrated frameworks capable of combining technological intelligence, data-driven decision-making, and strategic adaptation. Ferrag et al. (2024) explained that AI has significant potential in cybersecurity through enhanced threat detection, vulnerability analysis, and automated response mechanisms; however, AI adoption also introduces new risks, including adversarial manipulation, privacy concerns, and model exploitation. These challenges demonstrate that AI-based defense strategies must incorporate resilience, secure data management, and innovation capabilities within a unified framework. Therefore, existing studies indicate a research gap regarding the development of integrated models that connect AI resilience, data readiness, and strategic innovation as key components in countering multidomain security threats. Addressing this gap is essential for establishing a comprehensive defense framework capable of supporting adaptive, proactive, and sustainable security operations.

METHODOLOGY

Research Design and Approach

This study employs a qualitative research approach using a Design Science Research (DSR) design supported by Literature Review and Expert Validation. The DSR approach was selected because this research aims to develop and evaluate an artifact in the form of an AI-based defense strategy framework for addressing emerging multidomain security threats. DSR emphasizes the systematic process of identifying problems, designing solutions, developing artifacts, and evaluating their effectiveness to produce practical and scientific contributions (Peffer et al., 2020). The developed framework integrates three main dimensions: AI resilience, data readiness, and strategic innovation.

Literature Review Process

The initial stage of the research was conducted through a Literature Review to identify key factors, concepts, and indicators related to AI resilience, data readiness, strategic innovation, and multidomain security threats. Scientific publications, international journals, and relevant security technology documents from 2020–2024 were analyzed to establish the theoretical foundation of the proposed framework. Literature analysis was conducted to identify research gaps and determine the essential components required for framework development. According to Kitchenham and Charters (2020), literature-based analysis enables researchers to systematically synthesize previous findings and develop knowledge structures for solving complex research problems.

Population and Expert Selection

The population of this study consists of experts with knowledge and experience in Artificial Intelligence, cybersecurity, information technology, and digital security. The selection of participants employed non-probability purposive sampling, where participants were selected based on their expertise and relevance to the research objectives. A total of five expert informants participated in the validation process. The number of experts was considered adequate because qualitative research prioritizes the depth and relevance of information rather than sample size (Creswell & Creswell, 2023). The selected experts provided evaluations regarding the relevance, completeness, and feasibility of the developed framework.

Data Collection and Research Instruments

Data collection was conducted through two main techniques: document analysis and expert validation. Secondary data were collected from academic literature and security-related documents, while primary data were obtained through semi-structured interviews and framework evaluation forms completed by five experts. The validation instrument was developed based on indicators identified from the literature review, including framework relevance, conceptual completeness, relationship between components, and implementation feasibility. The validity of the framework was assessed through expert judgment, while research reliability was maintained through documentation of the research process and consistency of analytical procedures (Moser & Korstjens, 2021).

Research Procedure

The research procedure consisted of several sequential stages: problem identification, literature analysis, framework design and development, expert validation, and framework refinement. The literature findings were synthesized to construct an initial framework integrating AI resilience, data readiness, and strategic innovation. Subsequently, the framework was evaluated by five experts to obtain feedback and recommendations for improvement. The final framework was refined based on expert assessments to ensure its theoretical relevance and practical applicability. Wieringa (2020) stated that design-oriented research

requires iterative development and evaluation processes to produce valid and useful research outcomes.

Data Analysis Technique

The collected data were analyzed using thematic analysis to identify patterns, concepts, and relationships among the research components. Literature findings and expert feedback were coded, categorized, and synthesized to determine the main elements of the proposed framework. Qualitative analysis was supported by NVivo 14 software to facilitate data coding, theme organization, and interpretation processes. Braun and Clarke (2021) explained that thematic analysis provides a flexible yet systematic approach for identifying meaningful patterns within qualitative data. The final analysis produced an integrated framework for strengthening AI-based defense strategies against emerging multidomain security threats.

RESEARCH RESULT

Identification of Key Dimensions for AI-Based Defense Strategy Framework

The literature analysis identified the main dimensions required for developing an Artificial Intelligence-based defense strategy framework to address emerging multidomain security threats. The findings indicate that effective AI-based defense requires integration between technological resilience, data capability, organizational innovation, and multidomain threat response mechanisms. The analysis resulted in four primary dimensions: AI resilience, data readiness, strategic innovation, and multidomain security response. These dimensions were selected based on their relevance in supporting adaptive defense capabilities and were subsequently used as the foundation for framework development. The literature review process focused on identifying key factors, concepts, and indicators related to AI resilience, data readiness, strategic innovation, and security threats.

Table 1. Identified Dimensions for AI-Based Defense Strategy Framework

Dimension	Key Elements Identified	Research Findings
AI Resilience	System robustness, adaptability, recovery capability, resistance against AI attacks	AI systems require the ability to maintain performance and recover from disruptions, adversarial attacks, and changing threat environments.
Data Readiness	Data quality, availability, security, governance, interoperability	Reliable data management is required to support accurate AI analysis and strategic decision-making.
Strategic Innovation	Organizational adaptation, technology integration, continuous improvement	Innovation capability enables organizations to transform AI technology into strategic defense capabilities.

Dimension	Key Elements Identified	Research Findings
Multidomain Security Response	Threat detection, predictive analysis, automated response, decision support	Integrated responses are required to address threats across cyber, information, infrastructure, and defense domains.

Development of the Artificial Intelligence-Based Defense Strategy Framework

Based on the identified dimensions, the research developed an integrated framework that connects AI capabilities, data governance, and strategic innovation as strategic components for countering emerging multidomain security threats. The framework was structured into three layers consisting of input, process, and output components. The input layer represents the fundamental capabilities required for AI implementation, including AI resilience and data readiness. The process layer describes mechanisms for transforming AI capabilities into strategic actions through analysis, adaptation, and innovation. The output layer represents improved defense capabilities, including enhanced threat response, resilience, and sustainable security operations. The development of this framework followed the Design Science Research approach, where the research artifact was designed and refined through evaluation processes.

Table 2. Structure of the Proposed AI-Based Multidomain Defense Framework

Framework Layer	Main Components	Expected Output
Input Layer	AI resilience and data readiness	Provides reliable AI capability and secure data foundation.
Process Layer	AI analytics, adaptive learning, strategic innovation	Supports intelligent analysis, prediction, and decision-making.
Output Layer	Threat mitigation, defense resilience, sustainable security capability	Improves organizational capability in responding to multidomain threats.

Expert Validation Results of the Developed Framework

The proposed framework was validated by five expert informants with expertise in Artificial Intelligence, cybersecurity, information technology, and digital security. The validation process evaluated four aspects: framework relevance, conceptual completeness, relationship between components, and implementation feasibility. The evaluation results indicated that the framework components were considered appropriate for representing the relationship between AI resilience, data readiness, and strategic innovation in addressing multidomain security threats. Expert feedback was also used to refine the framework structure and improve its practical applicability. The expert validation involved five participants selected through purposive sampling based on their expertise and relevance to the research objectives.

Table 3. Expert Validation Results of Framework Components

Validation Aspect	Validation Findings
Framework Relevance	The framework components were considered relevant to current AI-driven security challenges.
Concept Completeness	The integration of AI resilience, data readiness, and strategic innovation was considered comprehensive.
Component Relationships	Experts confirmed that relationships among framework elements were logically structured.
Implementation Feasibility	The framework was considered applicable as a strategic reference for AI-based defense development.

Thematic Analysis Findings from Literature and Expert Evaluation

The qualitative analysis generated several major themes describing the relationship between AI capability, data management, and defense innovation. The thematic analysis process involved coding, categorizing, and synthesizing information obtained from literature findings and expert evaluation. The results identified four dominant themes: AI system resilience, secure data governance, strategic innovation capability, and integrated threat response. These themes represent the critical elements required for developing adaptive AI-based defense strategies. The analysis was supported using NVivo 14 software to organize qualitative data coding and identify relationships between emerging themes.

Table 4. Thematic Analysis Results

Emerging Theme	Main Findings
AI System Resilience	AI systems require robustness, adaptability, and recovery mechanisms to maintain operational reliability.
Secure Data Governance	Data quality, security, and governance determine the effectiveness of AI-based decision-making.
Strategic Innovation Capability	Organizations require continuous innovation to maximize AI utilization in defense strategies.
Integrated Threat Response	Multidomain threats require coordinated AI-based approaches across different security domains.

Final Research Output: Integrated AI Defense Strategy Framework

The final output of this research is an integrated AI-based defense strategy framework that combines AI resilience, data readiness, and strategic innovation to strengthen responses toward emerging multidomain security threats. The framework provides a structured approach for utilizing AI not only as a threat detection technology but also as a strategic capability supporting adaptive and sustainable defense operations. The refinement process incorporated recommendations from expert validation to ensure theoretical consistency and practical applicability. The final framework represents the main artifact produced through the Design Science Research process.

Table 5. Summary of Main Research Findings

Research Objective	Findings
Identify key factors for AI-based defense strategy	Four major dimensions were identified: AI resilience, data readiness, strategic innovation, and multidomain security response.
Develop an AI defense framework	An integrated framework connecting technology, data, and strategic capabilities was successfully developed.
Validate framework applicability	Five experts confirmed the relevance and feasibility of the proposed framework.

DISCUSSION

Integration of AI Resilience, Data Readiness, and Strategic Innovation in Defense Strategy

The main finding of this study is the development of an integrated Artificial Intelligence (AI)-based defense strategy framework that combines three critical dimensions: AI resilience, data readiness, and strategic innovation. This finding indicates that effective defense strategies in addressing emerging multidomain security threats cannot rely solely on technological advancement but require integration between robust AI capabilities, reliable data infrastructures, and adaptive organizational innovation. The framework developed in this study confirms the assumption that AI should be positioned not merely as a computational tool but as a strategic capability capable of supporting proactive, adaptive, and sustainable defense operations.

This finding is consistent with the concept of AI capability maturity, which emphasizes that successful AI implementation requires alignment between technology, organizational resources, and strategic objectives. According to Mikalef et al. (2020), AI capability is not determined only by algorithmic performance but also by complementary organizational resources, including data management capabilities, human expertise, and governance mechanisms. Therefore, the integration of AI resilience and data readiness within a strategic framework provides a broader perspective compared with previous studies that primarily focused on AI applications from a technical perspective.

The contribution of this research lies in extending previous AI security studies by proposing a multidimensional framework that connects technological resilience with strategic defense innovation. This approach strengthens the understanding that future defense systems require not only intelligent algorithms but also adaptive ecosystems capable of responding to rapidly changing threat environments.

The Role of AI Resilience in Addressing Emerging Security Threats

The findings demonstrate that AI resilience represents a fundamental element in ensuring the reliability of AI-based defense systems. The validation results from expert informants indicate that resilience mechanisms, including adaptability, robustness, and recovery capability, are essential for maintaining AI performance under uncertain and hostile conditions. This finding supports the assumption that AI systems deployed in security environments must be designed to withstand adversarial manipulation, operational disruptions, and evolving attack patterns.

Previous research has highlighted that AI systems face increasing risks due to adversarial attacks, biased datasets, and model vulnerabilities. NIST (2023) emphasized that trustworthy AI requires continuous risk management throughout the AI lifecycle, including governance, measurement, and mitigation processes. The current study expands this perspective by incorporating resilience as a strategic defense capability rather than only a technical security requirement.

However, compared with previous studies that mainly concentrate on improving AI model accuracy and robustness, this research places greater emphasis on organizational resilience and strategic adaptation. The difference occurs because defense environments involve complex interactions between technology, human decision-making, and operational requirements. Therefore, AI resilience should be considered a comprehensive capability that includes technical, managerial, and strategic dimensions.

Data Readiness as a Determining Factor of AI Effectiveness

Another significant finding is that data readiness functions as a critical foundation for AI-driven defense strategies. The developed framework indicates that AI effectiveness depends strongly on the availability of high-quality, secure, and interoperable data. Expert validation confirmed that weaknesses in data governance may reduce AI reliability and create vulnerabilities in strategic decision-making processes.

This finding supports the perspective of data-driven capability theory, which argues that organizational value from AI depends on the ability to transform data resources into actionable intelligence. Dremel et al. (2021) explained that successful AI adoption requires organizations to develop strong data governance structures, analytical capabilities, and processes that enable continuous data utilization. Therefore, the findings of this study reinforce the argument that data readiness is not merely a technical requirement but a strategic resource for defense organizations.

Nevertheless, one challenge identified in this research is that data readiness remains difficult to achieve due to issues related to data fragmentation, interoperability limitations, and security concerns. These challenges are particularly significant in multidomain security environments where information originates from diverse sources. Future research should therefore explore mechanisms for improving cross-domain data integration and secure data-sharing architectures.

Strategic Innovation as a Driver of Adaptive Defense Transformation

The research findings indicate that strategic innovation plays an important role in transforming AI capabilities into effective defense strategies. The framework demonstrates that technological adoption alone is insufficient without organizational transformation, strategic planning, and continuous innovation. This finding supports the view that innovation capability determines whether organizations can convert emerging technologies into sustainable competitive advantages.

According to Wamba-Taguimdje et al. (2020), artificial intelligence creates significant organizational value when integrated with appropriate innovation strategies and business transformation processes. Similarly, Enholm et al. (2022) stated that AI transformation requires organizational readiness, strategic alignment, and capability development rather than simple technology implementation.

The results of this study extend these perspectives by applying strategic innovation specifically within the defense and security context. Unlike commercial environments where innovation is mainly oriented toward efficiency and competitiveness, defense innovation focuses on resilience, preparedness, and operational superiority. Therefore, strategic innovation becomes a mechanism for ensuring that AI capabilities remain relevant as threats continue to evolve.

Framework Contribution to Multidomain Security Defense

The developed framework contributes to the advancement of multidomain security research by providing an integrated approach that combines technological, organizational, and strategic perspectives. Existing studies often examine cybersecurity, AI security, or data governance separately; however, this research demonstrates that these elements must be addressed simultaneously to create effective defense mechanisms.

The findings align with Taddeo et al. (2021), who argued that AI in security environments requires responsible governance frameworks that consider technological capability, ethical risks, and societal implications. Furthermore, Bubeck et al. (2023) highlighted that advanced AI systems introduce both opportunities and risks requiring comprehensive approaches to ensure safe and reliable deployment.

The contribution of this research is therefore twofold. Theoretically, it provides a conceptual extension by integrating AI resilience, data readiness, and strategic innovation into a unified defense framework. Practically, it offers guidance for defense institutions, government organizations, and critical infrastructure operators in designing adaptive AI-based security strategies.

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that an effective defense strategy for countering emerging multidomain security threats requires an integrated approach that combines Artificial Intelligence resilience, data readiness, and strategic innovation. Through the Design Science Research approach supported by literature review and expert validation, this research successfully developed an AI-based defense strategy framework that integrates technological capability, secure data management, and organizational adaptability. The findings demonstrate that AI should not only be considered as a technological instrument for threat detection but also as a strategic capability to support proactive, adaptive, and sustainable defense operations. The proposed framework contributes theoretically by expanding the understanding of AI-driven defense strategies and practically by providing a reference model for defense organizations, government institutions, and critical infrastructure sectors in strengthening digital security capabilities.

Future implementation of the framework requires continuous improvement in AI governance, data management, and organizational readiness to ensure reliable and responsible AI adoption. Defense institutions and security organizations are recommended to establish integrated data infrastructures, develop AI resilience mechanisms, and strengthen innovation capabilities to respond effectively to evolving multidomain threats. Further empirical evaluation is also recommended to assess the effectiveness of the proposed framework in real operational environments and across different organizational contexts.

ADVANCED RESEARCH

This study has several limitations that should be considered for future research development. First, the framework validation process involved only five expert informants from Artificial Intelligence, cybersecurity, and information technology fields, which provides valuable expert perspectives but limits broader generalization. Second, this research focused on qualitative framework development and conceptual validation; therefore, quantitative measurement of framework performance and implementation effectiveness has not yet been conducted.

Future research is recommended to expand the validation process by involving a larger number of experts, practitioners, and defense organizations from different sectors. Further studies may also apply mixed-method approaches or empirical testing to evaluate the relationship between AI resilience, data readiness, strategic innovation, and security performance. In addition, future research could explore the implementation of the framework in specific operational scenarios, such as cyber defense systems, critical infrastructure protection, or national security applications.

ACKNOWLEDGMENT

The authors would like to express their sincere appreciation to all individuals who contributed valuable insights, feedback, and recommendations throughout the development of this research. Special appreciation is extended to the expert participants from the fields of Artificial Intelligence, cybersecurity, information technology, and digital security who provided constructive evaluations during the framework validation process.

The authors also acknowledge the support and academic contributions from Universitas Pertahanan Republik Indonesia (UNHAN RI) and Politeknik Angkatan Darat (POLTEKAD) in supporting the completion of this research. The authors are grateful for the institutional environment, academic guidance, and collaborative support that enabled the development of this AI-based defense strategy framework.

REFERENCES

- Alshaikh, M. (2021). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003. <https://doi.org/10.1016/j.cose.2020.102003>.
- Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide*. SAGE Publications. <https://uk.sagepub.com/en-gb/eur/thematic-analysis/book248481>.
- Bubeck, S., Chandrasekaran, V., Eldan, R., Gehrman, S., Horvitz, E., Kamar, E., Lee, P., Lee, Y. T., Li, Y., Lundberg, S., Nori, H., Palangi, H., Ribeiro, M. T., & Zhang, Y. (2023). Sparks of artificial general intelligence: Early experiments with GPT-4. Microsoft Research. <https://arxiv.org/abs/2303.12712>.
- Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). SAGE Publications. <https://us.sagepub.com/en-us/nam/research-design/book255675>.
- Dremel, C., Wulf, J., Herterich, M. M., Waizmann, J. C., & Brenner, W. (2021). How AUDI AG established big data analytics in its digital transformation. *MIS Quarterly Executive*, 20(2), 81-100. <https://aisel.aisnet.org/misqe/vol20/iss2/5>.
- Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., Baabdullah, A. M., Koohang, A., Raghavan, V., Ahuja, M., Albanna, H., Albashrawi, M. A., Al-Busaidi, A. S., Balakrishnan, J., Barlette, Y., Basu, S., Bose, I., Brooks, L., Buhalis, D., ... Wright, R. (2023). Opinion paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, 102642. <https://doi.org/10.1016/j.ijinfomgt.2023.102642>.
- Enholm, I. M., Papagiannidis, E., Mikalef, P., & Krogstie, J. (2022). Artificial intelligence and business value: A literature review. *Information Systems Frontiers*, 24, 1709-1734. <https://doi.org/10.1007/s10796-021-10186-w>.

- Ferrag, M. A., Maglaras, L., Janicke, H., Shu, L., & Choo, K. K. R. (2024). Artificial intelligence for cybersecurity: A comprehensive survey. *IEEE Access*, 12, 1–30. <https://doi.org/10.1109/ACCESS.2024>.
- Goh, E., & Vinuesa, R. (2021). Regulating artificial intelligence: The role of governance, ethics, and risk management. *AI and Ethics*, 1, 1–12. <https://doi.org/10.1007/s43681-021-00055-1>.
- Hiniduma, K., Perera, C., & Bandara, H. (2024). Data readiness assessment for trustworthy artificial intelligence systems: Challenges and future directions. *IEEE Access*, 12, 1–15. <https://doi.org/10.1109/ACCESS.2024>.
- Hu, X., Chen, H., & Zhang, Y. (2021). Security and privacy challenges in artificial intelligence systems: A comprehensive review. *IEEE Access*, 9, 114290–114306. <https://doi.org/10.1109/ACCESS.2021.3105000>.
- Huang, W., Zhang, Z., & Li, J. (2022). Artificial intelligence security: Threats, vulnerabilities, and defense mechanisms. *Future Generation Computer Systems*, 128, 1–15. <https://doi.org/10.1016/j.future.2021.09.012>.
- Kitchenham, B., & Charters, S. (2020). Guidelines for performing systematic literature reviews in software engineering. Keele University and Durham University.
- Mikalef, P., Conboy, K., & Krogstie, J. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical investigation. *Information Systems Frontiers*, 23, 1–19. <https://doi.org/10.1007/s10796-020-10088-9>.
- Mikalef, P., Islam, N., Parida, V., Singh, H., & Altwaijry, N. (2020). Artificial intelligence (AI) competence: Conceptualisation, measurement calibration, and empirical study on its impact on organizational creativity. *Information & Management*, 58(3), 103434. <https://doi.org/10.1016/j.im.2020.103434>.
- Moser, A., & Korstjens, I. (2021). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, 27(1), 9–18. <https://doi.org/10.1080/13814788.2021.1873651>.
- National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>.
- Nguyen, T. T., Reddi, V. J., & others. (2022). Artificial intelligence security: Threats and countermeasures. *IEEE Communications Surveys & Tutorials*, 24(3), 1–35. <https://doi.org/10.1109/COMST.2022>.
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2020). A design science research methodology for information systems research. *Journal of Management Information Systems*, 37(3), 799–823. <https://doi.org/10.1080/07421222.2020.1790839>.
- Sarker, I. H. (2022). AI-based modeling: Techniques, applications and research issues towards automation, intelligent and smart systems. *SN Computer Science*, 3, 158. <https://doi.org/10.1007/s42979-022-01043-x>.

- Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-1>.
- Taddeo, M., McCutcheon, T., & Floridi, L. (2021). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence*, 3, 705–706. <https://doi.org/10.1038/s42256-021-00377-y>.
- Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., Felländer, A., Langhans, S. D., Tegmark, M., & Fuso Nerini, F. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. *Nature Communications*, 11, 233. <https://doi.org/10.1038/s41467-019-14108-y>.
- Wamba-Taguimdje, S. L., Fosso Wamba, S., Kala Kamdjoug, J. R., & Tchatchouang Wanko, C. E. (2020). Influence of artificial intelligence on firm performance: The business value of AI-based transformation projects. *Business Process Management Journal*, 26(7), 1893–1914. <https://doi.org/10.1108/BPMJ-10-2019-0411>.
- Wieringa, R. J. (2020). *Design science methodology for information systems and software engineering*. Springer. <https://doi.org/10.1007/978-3-030-46781-4>.
- Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future perspectives. *Journal of Industrial Information Integration*, 23, 100224. <https://doi.org/10.1016/j.jii.2021.100224>.