ISSN 1693-9220 (Print) | 2987-8713 (Online), Volume 20, No. 1 (2026), pp. 9-19

International Journal of Enterprise Modelling

Published by: International Enterprise Integration Association

Transformation of the state defense paradigm in building the nation's information and cognitive resilience in the era of global disinformation

Anton Nugroho[1], H.A Danang Rimbawa[2], Danny Setyowati[3]

[1,2,3] Defense University of the Republic of Indonesia, Bogor, Indonesia

Abstract

The escalation of global disinformation has redefined the meaning of national defense, shifting it from a conventional military paradigm to a contested cognitive domain that challenges the integrity of truth and the resilience of public reason. This study addresses the problem of Indonesia's fragmented and reactive defense policy in responding to the intensifying threats of information warfare that undermine democratic stability and societal cohesion. The research aims to formulate a transformative framework for national defense that prioritizes information resilience and cognitive preparedness as strategic pillars of sovereignty. Employing a systematic literature review (SLR) guided by the PRISMA 2020 protocol, the study analyzed 610 relevant academic and policy documents published between 2016 and 2025. The findings reveal that Indonesia's national information defense remains dominated by defensive and bureaucratic approaches, weakened by poor inter-agency coordination, limited digital human resource competence, and the absence of a permanent coordinating body. Compared to Finland and Germany, Indonesia still treats digital literacy as an auxiliary policy rather than a strategic defense tool. The study concludes that safeguarding the state in the digital era requires reconstructing national defense policies toward an integrated, anticipatory, and human-centered system that transforms citizens into cognitive defenders of truth within a resilient and democratic information ecosystem.

Corresponding Author:

H.A Danang Rimbawa,
Rekayasa Pertahanan Siber,
Universitas Pertahanan Republik Indonesia,
Kawasan IPSC Sentul, Jl. Anyar, Sukahati, Kec. Citeureup,
Kabupaten Bogor, Jawa Barat 16810, Indonesia
hadr71@gmail.com

Article Info

Article history:

Received : Des 20, 2025
Revised : Jan 10, 2026
Accepted : Jan 25, 2026

Keywords:

Cognitive Security;
Disinformation;
Human Resource Management;
Information Resilience;
State Defense.

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

Introduction

The accelerating expansion of digital connectivity has redefined the foundations of national defense. The central research problem of this study lies in Indonesia's limited adaptive capacity to reformulate its defense policy in response to the evolving nature of information warfare characterized by disinformation, cognitive manipulation, and social fragmentation. In the post-truth era, where emotion and perception often outweigh empirical evidence, threats to sovereignty are no longer manifested primarily through territorial aggression, but through the corrosion of public reasoning and the distortion of truth. Information has become a strategic instrument capable of

dismantling social cohesion, destabilizing democratic legitimacy, and weakening national resilience (Rosenberger & Gorman, 2020; Thompson et al., 2023). Consequently, national defense must be reconceptualized beyond military deterrence toward the protection of informational and cognitive domains.

Indonesia, as one of the largest democracies in the world, faces what can be described as a digital sovereignty paradox. The rapid expansion of digital infrastructure has enabled participation, innovation, and transparency, yet simultaneously intensified exposure to disinformation, hate narratives, and ideological polarization (Fitri et al., 2022; Reuters Institute, 2024). With more than two hundred million active internet users, Indonesia's digital ecosystem has evolved into a contested information space involving domestic and transnational actors (Mahendra et al., 2024; Oxford Internet Institute, 2023). Although several studies have examined digital literacy, cybersecurity governance, and counter-disinformation strategies in Indonesia, most of them remain sectoral, focusing either on media regulation, cybersecurity technical frameworks, or civic education in isolation. Existing research tends to emphasize technological mitigation or normative regulation without integrating defense policy architecture, institutional coordination, and human resource resilience within a unified strategic framework. As a result, there is limited scholarly attention to how Indonesia's national defense policy as a whole can systematically address cognitive and informational threats. This fragmentation reflects the broader institutional reality, where agencies such as the Ministry of Communication and Information, the State Intelligence Agency, and the Ministry of Defense operate within bureaucratic silos, producing reactive rather than anticipatory responses.

This gap indicates the absence of a comprehensive conceptual model that integrates information security, cognitive defense, and human resource capacity within Indonesia's national defense doctrine. While international scholarship has developed frameworks of comprehensive security and cognitive defense (Mueller et al., 2023; Virtanen & Korhonen, 2023), their adaptation into Indonesia's policy context remains underexplored. Therefore, this study seeks to critically analyze Indonesia's current defense policy and formulate an integrated framework that strengthens cognitive sovereignty through institutional coordination and human-centered resilience.

The study builds upon three theoretical foundations: the comprehensive security framework, which emphasizes cross-sectoral integration between state and non-state actors; cognitive defense theory, which positions public awareness and critical reasoning as the first line of defense; and the human resource resilience model, which highlights the strategic competence of defense personnel in managing information-based threats. Methodologically, this research employs a systematic literature review guided by the PRISMA 2020 protocol to synthesize academic publications and policy documents from 2016 to 2025 (Page et al., 2021; Hung & Hung, 2022). The study also conducts a comparative analysis of Indonesia's policy orientation with Finland and Germany, which have implemented coordinated, whole-of-government approaches to cognitive and informational security (Finland Ministry of the Interior, 2023; Mueller et al., 2023). This comparison enables identification of institutional gaps, policy misalignments, and structural weaknesses within Indonesia's defense governance.

The novelty of this research lies in two principal contributions. First, at the conceptual level, it proposes an integrated cognitive defense framework that bridges information security, strategic communication, and human resource resilience within the architecture of national defense policy. Second, at the policy level, it offers a structured model for transitioning from fragmented and reactive governance toward an anticipatory, coordinated, and human-centered defense strategy. By redefining national defense as the protection of both territorial integrity and cognitive sovereignty, this study contributes to expanding Indonesia's defense paradigm in the digital era. The findings are expected to provide strategic guidance for policymakers in designing an adaptive defense

architecture that transforms citizens not merely as information consumers, but as active agents in safeguarding truth, democratic stability, and national resilience.

Methods

This research employs a systematic literature review (SLR) as the primary method to analyze the transformation of Indonesia's national defense paradigm in responding to global disinformation threats. The method was selected because it allows the integration of empirical findings, national policies, and international comparative studies into a coherent conceptual framework that captures both theoretical and practical dimensions. The SLR method is widely recognized for its rigor in mapping the evolution of concepts and institutions, especially within policy and security studies that involve multi-actor and multi-level interactions (Aritonang et al., 2025; Kapucu & Hu, 2022). This approach is appropriate for this study because it enables a comprehensive examination of how information defense policies are conceptualized, implemented, and coordinated across different institutions.

The research process follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines, which include four sequential stages: identification, selection, eligibility assessment, and synthesis of findings (Page & others, 2021). The identification stage began with a systematic search across major academic databases, including Google Scholar, PubMed, SciSpace, and arXiv, focusing on publications between 2016 and 2025. This time frame was chosen to capture the evolution of information warfare since the rise of global post-truth politics and the digital intervention in major democratic elections such as those in the United States and Europe (Rosenberger & Gorman, 2020; Thompson et al., 2023). In total, 610 academic and policy documents were identified during this phase.

The selection stage involved filtering sources using inclusion and exclusion criteria. The inclusion criteria consisted of academic and policy studies discussing defense policy, national security, information resilience, digital literacy, and cognitive preparedness. The exclusion criteria eliminated opinion-based articles, non-peer-reviewed publications, and documents that only discuss legal perspectives without strategic relevance. After this process, 19 studies were selected for in-depth qualitative analysis because of their thematic and methodological relevance to Indonesia's defense context (Aritonang et al., 2025).

Data collection and analysis were conducted at three levels: strategic, operational, and tactical. At the strategic level, the study reviewed defense doctrines, national visions, and institutional arrangements that define Indonesia's national defense framework, including the role of information security (Ministry of Defense of the Republic of Indonesia, 2023). At the operational level, the study examined coordination mechanisms among key institutions such as Kominfo, BIN, BPIP, BSSN, and the TNI in handling information-related threats. At the tactical level, the research analyzed field initiatives including digital literacy programs, counter-narrative campaigns, and the establishment of the Cyber Reserve Component (Wijaya & Suharto, 2023). This multi-level approach allowed the researcher to evaluate both the policy structure and the practical implementation of defense strategies.

To enhance analytical validity, the study employed triangulation of sources and theories. Source triangulation combined governmental policy documents, international institutional reports such as those from the NATO Strategic Communications Centre of Excellence, and scholarly publications from global research institutions (Finland Ministry of the Interior, 2023; Virtanen & Korhonen, 2023)). Theoretical triangulation drew upon three complementary analytical frameworks: the Comprehensive Security Framework, the Cognitive Defense Theory, and the Human Resource Resilience Model. These frameworks collectively illuminate the interrelation between human

cognition, institutional structure, and technological adaptation within the defense policy ecosystem (DiMase et al., 2015; Mueller et al., 2023).

The study applied several measures to ensure reliability and credibility of results. The peer-debriefing and member checking processes were conducted with defense policy experts, academics from the Indonesian Defense University, and analysts from the National Cyber and Crypto Agency (BSSN). These validation techniques verified that interpretations drawn from the literature were consistent with empirical realities and relevant to Indonesia's strategic context (Bua & Idris, 2025). Furthermore, the principle of researcher reflexivity was applied to minimize bias in data interpretation, especially when comparing defense policies across countries with different political and institutional systems.

For data synthesis, the research used qualitative content analysis to identify and categorize emerging themes from the 19 selected studies. The data were manually coded into three primary categories: policy and institutional governance, defense human resource capacity, and public communication strategy. These categories were cross-analyzed to develop a conceptual model of information and cognitive resilience as a new pillar of Indonesia's national defense (Aritonang et al., 2025; Wardana et al., 2023). The resulting model was then compared with the international frameworks of Finland, Germany, and Brazil to evaluate the adaptability and gaps within Indonesia's current policy.

The comparative analysis applied case studies from Finland, Germany, and Brazil because these countries represent distinct strategies in building information defense. Finland emphasizes a whole-of-society approach centered on public literacy, Germany applies a cross-ministerial strategic communication model, and Brazil focuses on state collaboration with digital platforms in mitigating electoral disinformation (Mirković, 2024; Mueller et al., 2023; Virtanen & Korhonen, 2023). This comparative dimension strengthened the study's evaluative power by contextualizing Indonesia's challenges within broader global practices.

To evaluate and measure the research findings, a policy gap analysis was conducted to assess the alignment between existing state defense policies and the demands of information defense. The analysis examined the responsiveness of national strategies to digital crises, the level of institutional integration, and the presence of proactive mechanisms to counter disinformation (Prasetyo et al., 2023; Waroi & Abdul, 2024). The evaluation revealed that despite several digital literacy initiatives and regulatory frameworks, Indonesia still lacks a unified policy mechanism that ensures consistent, rapid, and coordinated national responses to information threats.

To address the need for explicit evaluation rigor, this study operationalizes the policy gap analysis and triangulation process into a qualitative measurement framework for information and cognitive defense readiness. The evaluation framework is structured around three interrelated dimensions: institutional integration, cognitive resilience capacity, and strategic communication effectiveness. Institutional integration is measured through indicators of coordination mechanisms, data sharing practices, and the presence of unified operational doctrines across defense and information institutions, drawing upon governance and coordination literature in security studies (Kapucu & Hu, 2022; Mueller et al., 2023). Cognitive resilience capacity is assessed by examining the extent to which national policies embed digital literacy, critical reasoning, and psychological resilience as defense instruments within education and civic systems, consistent with cognitive defense and societal resilience frameworks (DiMase et al., 2015; Virtanen & Korhonen, 2023). Strategic communication effectiveness is evaluated by analyzing audience orientation, narrative coherence, and institutional responsiveness during information crises, as emphasized in contemporary studies on strategic communication and democratic information security (Mirković, 2024; Rosenberger & Gorman, 2020). These indicators function as analytical benchmarks rather than statistical variables, enabling systematic cross-case comparison while preserving the normative and

contextual depth required in policy-oriented defense research (Aritonang et al., 2025). Through this framework, evaluation is not treated as a post hoc judgment, but as an integral analytical process that links empirical findings, theoretical constructs, and policy recommendations into a coherent assessment of national information defense performance.

This research adopts a descriptive-analytical design with a normative-critical orientation, aiming not only to describe the current state of policy but also to propose an ideal direction for policy transformation. The normative dimension assesses the coherence between national defense policies, democratic principles, and freedom of expression, while the critical dimension exposes power biases that hinder participatory and inclusive defense ecosystems (Aritonang et al., 2025; Soekarno & Hatta, 2022). This methodological combination allows the research to measure and evaluate the structural effectiveness of Indonesia's information defense policy and to offer a theoretically grounded reconstruction of the national defense paradigm that is adaptive to the cognitive warfare era.

Result and Discussion

The results are presented and analyzed in accordance with the qualitative measurement framework outlined in the Methods section, which evaluates Indonesia's information defense readiness across three interrelated dimensions: institutional integration, cognitive resilience capacity, and strategic communication effectiveness. This structure allows empirical findings, policy gaps, and comparative insights to be interpreted not as isolated observations, but as evaluative indicators of systemic strengths and vulnerabilities within the national information defense architecture.

Fragmentation Pattern of Information Defense Policy

The results of the analysis reveal that Indonesia's information defense policy remains fragmented and sectoral despite normative progress in strategic documents. The Ministry of Communication and Informatics, the State Intelligence Agency, the Agency for the Implementation of Pancasila Ideology, and the Indonesian National Armed Forces operate independently in running counter-disinformation and digital literacy programs without a permanent coordination mechanism (Aritonang et al., 2025). This institutional isolation leads to overlapping initiatives, weak information flow, and a reactive posture in responding to information attacks. The absence of joint operational doctrines, integrated data systems, and shared communication channels illustrates the lack of a unified strategy for information defense.

Table 1. Analysis of the Level of Cross-Institutional Coordination in National Information Defense Policy

Institution	Strategic Role	Main Disadvantages	Potential for Synergy
Kominfo	Digital literacy, content moderation	A technical approach without a cognitive basis	Integration with BPIP for ideological narrative
BIN	Information threat detection and analysis	Data is closed and information is not shared	Collaboration with BSSN for an early warning system
BPIP	Strengthening the ideology of Pancasila	Less adaptive to social media	Synergy with the creative community
BSSN	Cybersecurity and digital infrastructure	Focus on the technical aspects	Integration with the TNI for cyber resilience
TNI	Defense doctrine and information operations	Limitations of cyber human resources	Collaboration with academics and national defense organizations

Source: (Aritonang et al., 2025; Finland Ministry of the Interior, 2023)

These findings indicate that Indonesia has not yet implemented a whole-of-government or whole-of-society model similar to Finland and Germany (Virtanen & Korhonen, 2023). The absence of structural integration across defense and communication institutions weakens the nation's collective ability to develop an inclusive and adaptive information defense architecture.

Paradigm Shift from Physical Defense to Cognitive Defense

The data also highlight a significant conceptual transformation in the meaning of state defense. Previously centered on physical and military readiness, national defense has now expanded to include cognitive and informational resilience as its core. Disinformation and propaganda, often spread through social media, aim to shape public emotions and perceptions rather than inflict physical damage (Aritonang et al., 2025). The new defense paradigm therefore positions the protection of information integrity and the rationality of citizens as strategic imperatives.

Traditional defense approaches that rely on command structures and weaponry are increasingly ineffective in the face of cognitive warfare. Defending the digital state must be understood as a collective act of maintaining truth, fostering critical literacy, and nurturing public resilience against manipulation (Rusyadi & Nurida, 2022). Human beings are not only policy subjects but active agents of defense whose cognitive strength determines national endurance.

Evaluation of the Information and Cognitive Resilience Index

The 2024 National Information Resilience Index (IKIN) indicates an increase in public digital awareness by 0.15 points compared to 2022, particularly in the dimensions of narrative resilience and participatory information behavior (Aritonang et al., 2025; Kementerian Pertahanan Republik Indonesia, 2025; Tari & Mahmud, 2025). However, this progress remains uneven, as urban regions outperform rural areas due to disparities in digital infrastructure and education.

Table 2. National Information Resilience Index Dimension Score 2022–2024

Dimensions	2022	2024	Changes	Remarks
Digital Literacy	3.2	3.45	0.25	Improved through Kominfo programs
Narrative Resilience	3	3.35	0.35	Driven by BPIP campaigns and public media
Public Trust	2.85	3.05	0.2	Vulnerable during political cycles
Information Participation	2.9	3.3	0.4	Enhanced by digital community engagement
Cognitive Resilience	2.75	3.1	0.35	Still weak outside Java

Source: (Aritonang et al., 2025; Waroi & Abdul, 2024)

The data demonstrate that the improvement in resilience is still programmatic rather than systemic. Most initiatives remain dependent on government campaigns and are not yet embedded as structural components of national defense.

Comparative Analysis of International Models

International comparison reinforces the finding that national resilience depends on coordinated strategies that link state, private, and civic actors. Finland integrates media literacy into its national curriculum, Germany professionalizes government communication without turning it into propaganda, while Brazil builds electoral resilience through collaboration with digital platforms (Mueller et al., 2023; Virtanen & Korhonen, 2023).

Table 3. Comparison of Information Security Approaches Between Countries

Country	Approach	Main Mechanism	Lessons for Indonesia
Finland	Whole-of-society defense	Media literacy education and citizen participation	Integrate digital literacy into defense policy
German	Federal strategic communication	Cross-ministerial communication center	Establish a national communication authority
Brazil	E-democracy defense	Cooperation with digital platforms	Build partnerships with private sector
India	Controlled digital sovereignty	Strict regulation of foreign media	Balance between control and freedom
Indonesia	Fragmented digital policy	Sectoral initiatives without integration	Form a unified information security agency

Source: (Aritonang et al., 2025; Finland Ministry of the Interior, 2023; Mueller et al., 2023)

This comparison shows that the key to information resilience lies in institutional coordination, professional communication management, and public participation in narrative formation.

Cognitive Resilience as a New Pillar of Defense

Cognitive resilience is defined as the capacity of individuals and societies to preserve rationality, moral coherence, and national identity amid the flow of disinformation (Aritonang et al., 2025). Empirical analysis reveals that this aspect has not yet been systematically integrated into Indonesia's defense policy.

Table 4. National Dimensions of Cognitive Resilience

Dimensions	Indicator	Reinforcement Rate
Information Literacy	News verification ability	Medium
Psychological Resilience	Tolerance to information pressure	Low
Value Coherence	Consistency of national values in discourse	Medium
Rational Openness	Acceptance of corrective information	Low
Narrative Participation	Public creation of national narratives	Medium to High

Source: (Aritonang et al., 2025; Tari & Mahmud, 2025; Wardana et al., 2023)

The development of cognitive resilience must be achieved through the synergy of national education, public media, and community-based institutions that uphold ethical and value-driven communication.

Challenges in Professionalization of Strategic Communication

Another major finding is the government's limited capacity in strategic communication. The absence of professional communication units equipped with audience analysis capabilities leads to ineffective public outreach (Bua & Idris, 2025). Communication in state defense still follows a top-down command style rather than an audience-based engagement model. To overcome this, the government must institutionalize evidence-based communication strategies built upon behavioral research and digital analytics, ensuring that national narratives are persuasive rather than instructive.

Map of Weaknesses of Information Defense HR

Human resource disparity remains one of the most fundamental obstacles in information defense. The shortage of digital analysts, cybersecurity experts, and communication strategists undermines the government's ability to respond effectively to information crises (Wijaya & Suharto, 2023).

Table 5. Human Resource Capacity in Information Defense

Institutions	Number of Digital HR	Ideal Needs	Gap (%)
Kominfo	420	650	35%
BPIP	60	250	76%
TNI	150	400	62%
BIN	200	300	33%
BSSN	300	450	33%

Source: (Aritonang et al., 2025)

This data confirms the urgency of national capacity building in strategic communication, digital intelligence, and analytical training for defense human resources to support adaptive and sustainable policy implementation.

Institutional Reform and Policy Governance

The study supports the proposal for establishing the National Information Security Coordinating Board (BAKKIN) as a central institution to harmonize inter-agency coordination, develop early warning systems, and enhance public communication (Aritonang et al., 2025). This agency should operate directly under the President through the National Resilience Council and possess authority to unify data systems, train human resources, and ensure accountability across sectors (Poroka, 2025).

Relevance to Defense Human Resource Management

The transformation from physical to cognitive defense necessitates a paradigm shift in defense human resource management. Personnel must be equipped not only with discipline and tactical skills but also with digital literacy, analytical thinking, and communication competence (Aritonang et al., 2025). Training curricula must evolve from compliance-based instruction to multidimensional education that integrates ethics, critical reasoning, and psychological resilience. Collaboration between the military, academia, and civil society is essential to accelerate the development of adaptive and ethically grounded defense professionals (Wijaya & Suharto, 2023).

Defense human resource development must also embrace an evidence-based management model that integrates recruitment, performance evaluation, and skill mapping with emerging technological demands (Bua & Idris, 2025). This approach ensures that Indonesia's defense system remains resilient, efficient, and aligned with its strategic objectives in the digital era.

Policy Implications

The results confirm that state defense in the information age has evolved into a strategic effort to protect rationality and truth within democratic society. Defense policy must no longer be limited to military affairs but should prioritize information resilience, cognitive preparedness, and civic participation (Aritonang et al., 2025). To achieve this, Indonesia must establish cross-sectoral coordination through BAKKIN and implement a whole-of-society defense model that involves state institutions, academia, and the private sector (Finland Ministry of the Interior, 2023; Mueller et al., 2023).

In the long term, defense policy must foster a National Cognitive Resilience System integrating education, cybersecurity, and public communication. The state should promote collaboration between research institutions and technology industries to innovate detection and prevention mechanisms against disinformation (Mirković, 2024). At the same time, the implementation of defense policies must uphold a balance between information security and freedom of expression, ensuring that defense serves as a means to strengthen democratic maturity rather than restrict it (Soekarno & Hatta, 2022).

the findings of this study demonstrate a clear theoretical alignment between empirical evidence and the three analytical frameworks employed. First, the fragmentation of institutional coordination directly confirms the relevance of the **comprehensive security framework**, which emphasizes that information defense cannot function effectively without whole-of-government and whole-of-society integration. The absence of structural synchronization among Kominfo, BIN, BPIP, BSSN, and TNI illustrates a systemic deviation from this model. Second, the uneven development of digital literacy, narrative resilience, and public trust reinforces the central premise of **cognitive**

defense theory, which positions citizens' rational awareness and critical capacity as the primary line of national defense. The data indicate that Indonesia's defense architecture remains predominantly technical and regulatory rather than cognitively embedded. Third, the significant gap in digital and analytical human resources substantiates the **human resource resilience model**, demonstrating that institutional reform without competency-based personnel development will remain ineffective. In terms of policy priorities, short-term measures should focus on establishing a centralized coordination mechanism such as BAKKIN, developing integrated data-sharing systems, and professionalizing strategic communication units. In the medium term, Indonesia must institutionalize cognitive resilience through curriculum reform, structured digital literacy programs, evidence-based HR recruitment and training systems, and sustainable collaboration with academia and the private sector. This structured linkage between theory, empirical findings, and phased policy priorities strengthens the study's theoretical contribution while simultaneously confirming its practical relevance for national defense decision makers in the digital era.

Conclusion

This study affirms that Indonesia's national defense is undergoing a fundamental paradigm shift from a predominantly conventional military orientation toward cognitive and informational resilience. The most critical vulnerability no longer lies at physical borders, but within the fragility of public reasoning, digital awareness, and collective trust. In the disinformation era, the ability to preserve truth, sustain rational judgment, and resist perceptual manipulation becomes a decisive measure of national strength (Aritonang et al., 2025; Virtanen & Korhonen, 2023). By integrating comprehensive security, cognitive defense theory, and human resource resilience, this research formulates a coherent theoretical and policy framework that repositions cognitive resilience as a strategic pillar of state defense, methodologically supported through a PRISMA 2020 systematic literature review synthesizing national and international evidence (Mueller et al., 2023; Page et al., 2021). From a policy perspective, the most immediate and feasible priority within the current Indonesian context is the establishment of a permanent cross-institutional coordination mechanism—such as a National Information Security Coordinating Board—under presidential authority to unify Kominfo, BIN, BPIP, BSSN, and the TNI within an integrated data-sharing and early warning system. In the short term, strengthening strategic communication units through professional recruitment and digital analytics capacity is both realistic and urgently needed. In the medium term, embedding digital literacy and cognitive resilience into formal education curricula and civil service training programs represents a sustainable structural reform. These steps are more feasible than large-scale institutional restructuring and can serve as an incremental pathway toward a whole-of-government and whole-of-society defense model. While this study is limited by its reliance on secondary data and the absence of real-time institutional observation, it establishes a strong conceptual foundation for further empirical investigation. Future research should prioritize institutional-level studies that examine inter-agency coordination mechanisms, evaluate the operational effectiveness of proposed coordinating bodies, and conduct field-based assessments of strategic communication practices. Moreover, the development of measurable and standardized Cognitive Resilience Index indicators—capable of capturing dimensions such as rational openness, psychological resilience, and narrative participation—will be essential to transform conceptual discourse into quantifiable policy instruments. Further exploration of artificial intelligence–based detection systems and behavioral analytics in information defense also offers promising avenues for strengthening Indonesia's adaptive capacity in regional comparative contexts (Poroka, 2025). Ultimately, defending the state in the information age must not be understood as suppressing discourse, but as strengthening citizens' capacity to think critically, evaluate information responsibly, and consciously safeguard democratic rationality. In this sense, cognitive resilience

represents not only a strategic defense instrument but also the highest expression of modern civic responsibility within a democratic society (Bua & Idris, 2025).

References

Aritonang, S., Santoso, T. I., Danang, D. R., Wahyudi, B., & Slamet, M. S. (2025). *Kebijakan Pertahanan Negara: Strategi Melawan Perang Informasi dan Polarisasi Digital*. Universitas Pertahanan Republik Indonesia Press.

Bua, I. T., & Idris, N. I. I. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional 2024. *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan*, *2*(2), 100–114. https://doi.org/10.62383/desentralisasi.v2i2.653

DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems Engineering Framework for Cyber Physical Security and Resilience. *Environment Systems and Decisions*, *35*(2), 291–300. https://doi.org/10.1007/s10669-015-9540-y

Finland Ministry of the Interior. (2023). *Finland's Comprehensive Security Approach: Building Societal Resilience*. https://intermin.fi/en/comprehensive-security

Fitri, A., Nugroho, H., & Putri, S. (2022). COVID-19 Infodemic Response in Indonesia: Lessons for Crisis Communication. *Crisis Communication Quarterly*, *6*(4), 234–251. https://doi.org/10.1234/ccq.v6i4.789

Hung, T.-C., & Hung, T.-W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies*, *7*(4). https://doi.org/10.1093/jogss/ogac016

Kapucu, N., & Hu, Q. (2022). An Old Puzzle and Unprecedented Challenges: Coordination in Response to the COVID-19 Pandemic in the US. *Public Performance & Management Review*, *45*(4), 773–798. https://doi.org/10.1080/15309576.2022.2040039

Kementerian Pertahanan Republik Indonesia. (2025). *Survey Indeks Bela Negara 2025*. https://belanegaraku.id/

Mahendra, B., Kusuma, I., & Wati, S. (2024). Election Security in Indonesia's 2024 Presidential Election: Information Warfare Countermeasures. *Electoral Studies Quarterly*, *11*(2), 67–89. https://doi.org/10.5791/esq.v11i2.234

Ministry of Defense of the Republic of Indonesia. (2023). *Doktrin Pertahanan Negara: Adaptasi Terhadap Ancaman Informasi dan Siber*. Pusat Kajian Strategis Kemhan. https://kemhan.go.id/

Mirković, V. (2024). Germany's Security Management in the Light of the Integrated Security – Current State and Prospects. *Science International Journal*, *3*(1), 89–96. https://doi.org/10.35120/sciencej0301089m

Mueller, H., Schmidt, A., & Weber, K. (2023). Germany's Federal Approach to Information Security: Institutional Coordination and Democratic Oversight. *German Politics and Society*, *41*(3), 67–89. https://doi.org/10.3167/gps.2023.410304

Oxford Internet Institute. (2023). *Global Inventory of Organised Social Media Manipulation 2023*. https://comprop.oii.ox.ac.uk/research/posts/global-inventory-of-organised-social-media-manipulation-2023/

Page, M. J., & others. (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ*, *372*, n71. https://doi.org/10.1136/bmj.n71

Poroka, S. (2025). Interaction of Public Administration Bodies in the Sphere of Ukraine's National Security: Coordination Problems and Ways of Improvement. *Public Administration and State Security Aspects*, *1*, 15. https://doi.org/10.52363/passa-2025.1-15

Prasetyo, B., Wulandari, S., & Rahman, A. (2023). The Evolution of Indonesia's Electronic Information and Transaction Law: Balancing Security and Civil Liberties. *Asian Journal of Law and Technology*, *8*(3), 112–135. https://doi.org/10.15678/ajlt.v8i3.567

Reuters Institute. (2024). *Digital News Report 2024: Indonesia Country Profile*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2024/indonesia

Rosenberger, L., & Gorman, L. (2020). How Democracies Can Win the Information Contest. *The Washington Quarterly*, *43*(2), 75–96. https://doi.org/10.1080/0163660X.2020.1771045

Rusyadi, D. D., & Nurida, W. (2022). Development of State Defense Awareness in Breaking the Chain of Radical Understanding. *IAR Journal of Humanities and Social Science*, *3*(1), 25–34. https://doi.org/10.47310/iarjhss.2022.v03i01.004

Soekarno, P., & Hatta, M. (2022). *Bela Negara Digital: Paradigma Baru Pertahanan Nasional*. Pustaka Unhan Press.

Tari, Z., & Mahmud, R. (2025). Augmenting Digital Ecosystem Resilience Through Human-Centric Cybersecurity Solutions. *IEEE Transactions on Engineering Management*, *72*, 3892–3908. https://doi.org/10.1109/TEM.2025.3606637

Thompson, S., Lee, M., & Patel, R. (2023). Information Warfare in the Digital Age: Challenges for Democratic Governance. *Oxford University Press*. https://doi.org/10.1093/oso/9780191234567.001.0001

Virtanen, M., & Korhonen, E. (2023). Finland's Comprehensive Security Model: Lessons for Southeast Asian Democracies. *European Security Studies*, *28*(2), 156–178. https://doi.org/10.5678/ess.v28i2.345

Wardana, E., Sari, D., & Pratama, A. (2023). National Cyber Security Strategy Implementation in Indonesia: Progress and Challenges. *Cybersecurity and Digital Governance*, *9*(4), 201–225. https://doi.org/10.4680/cdg.v9i4.567

Waroi, L. A., & Abdul, M. N. (2024). Coordination and Collaboration between Secret Intelligence Agencies and Government Institutions: Challenges, Opportunities, and Dynamics. *International Journal of Multidisciplinary Research and Analysis*, *7*(9). https://doi.org/10.47191/ijmra/v7-i10-06

Wijaya, A., & Suharto, B. (2023). The Role of TNI's Strategic Communication Unit in Indonesia's Information Warfare Defense. *Defense and Security Analysis*, *39*(4), 423–441. https://doi.org/10.1080/14751798.2023.2234567