Nusantara: Journal of Law Studies
Vol. 5 No. 1, 2026: 582-601
E-ISSN: 2964-3384
https://doi.org/10.66325/nusantaralaw.v5i1.296

National Security Complex and Networked Securitization in Cognitive Warfare

Alzaki Alzaki[1]*, Arfin Sudirman[2], R. Widya Setiabudi Sumadinata[3], Wawan Budi Darmawan[4], Ola Madallah Aljaafreh[5]

[1,2,3,4] Faculty of Social and Political Sciences, Universitas Padjadjaran, Indonesia
[5]Ajloun National University, Ajloun, Jordan

DOI: doi.org/10.66325/ law.v5i1.296
*Corresponding Author: alzaki23001@mail.unpad.ac.id

Received: 09-01-2026 | *Revised: 13-04-2026* | *Accepted: 21-05-2026* | *Published On: 29-05-2026*

Abstract: This article examines how cognitive warfare is securitized in Indonesia amid technological disruption and strategic competition in the Indo-Pacific region. Drawing on securitization theory, Just Securitization Theory, and Regional Security Complex Theory (RSCT), the study develops a multilevel analytical framework that connects global, regional, and domestic dynamics. Methodologically, it employs qualitative document analysis of defense policies, doctrinal publications, and relevant academic literature. The findings demonstrate that securitization in Indonesia is best understood as a networked and institutionally distributed process involving political leaders, military organizations, intelligence agencies, cybersecurity bodies, regulatory institutions, and societal actors. The study identifies an expansion of referent objects, extending beyond territorial sovereignty to include democracy, information sovereignty, social cohesion, and ideological stability. It further shows that cognitive warfare has shifted the primary battlespace toward perception, narrative construction, and psychological influence. As a key theoretical contribution, the article introduces the concept of the National Security Complex to capture intra-state dynamics of securitization. This framework reveals that securitization is not only multilevel but also multi-centered within the state apparatus. The study concludes that, although the securitization of cognitive threats is becoming increasingly institutionalized, it remains constrained by normative tensions concerning civil liberties and democratic accountability. By proposing the concept of the National Security Complex, this article also addresses a theoretical gap in RSCT, which has traditionally emphasized inter-state dynamics, thereby enabling a more structured understanding of security contestation at the domestic level.

Keywords: Cognitive Warfare; Indo-Pacific Security; Information Warfare; National Security Complex; Securitization Theory.

Introduction

The transformation of contemporary conflict has shifted the primary terrain of security from the physical to the cognitive realm[1]. In the 21st-century strategic environment, power is no longer exercised solely through territorial control or military superiority, but also through the ability to influence perceptions, public opinion, emotions, and societal decision-making processes[2]. This phenomenon is known as cognitive warfare, a form of conflict that seeks to shape how individuals and groups perceive reality through the manipulation of information, narratives, and the digital environment[3]. Developments in digital technology—including social media, artificial intelligence, big data analytics, and algorithm-based information distribution systems—have enabled influence operations to be carried out on a massive scale, quickly, and precisely, making the information space a new strategic arena in global contestation.[4]

This development is increasingly relevant in the context of the Indo-Pacific, a region now at the center of strategic competition between the United States and China[5]. The competition between these two great powers is not only military and economic, but also in the struggle for normative influence, digital infrastructure, and the dominance of regional narratives through frameworks such as the Free and Open Indo-Pacific (FOIP) and the Belt and Road Initiative (BRI).[6] In this environment, disinformation operations, digital propaganda, and psychological influence have become integral parts of gray zone strategies, where both state and non-state actors seek to influence political and social orientations without crossing the threshold of open warfare[7]. Thus, cognitive warfare has become a crucial dimension of Indo-Pacific regional security[8].

In this context, Indonesia presents a highly strategic case for the study of cognitive warfare[9]. Indonesia's position as the largest democracy in Southeast Asia and a middle power in the Indo-Pacific region places it at the intersection of various global

---

[1] Igor F. Kefeli, Roman S. Vykhodets, and Olga V Plebanek, "Updating Cognitive Security in a Global Dimension," *Journal of Globalization Studies* 16, no. 1 (2025): 39–46.

[2] Keith Krause and Oliver Jütersonke, "Peace, Security and Development in Post-Conflict Environments," *Security Dialogue* 36, no. 4 (2005): 447–462.

[3] Barry Buzan, "New Patterns of Global Security in the Twenty-First Century," *International Affairs (Royal Institute of International Affairs 1944-)*, 1991, 431–451.

[4] Emanuel Adler, "Cognitive Evolution: A Dynamic Approach for the Study of International Relations and Their Progress," *Progress in Postwar International Relations* 43 (1991): 56.

[5] Muhammad Saeed, "From the Asia-Pacific to the Indo-Pacific: Expanding Sino-US Strategic Competition," *China Quarterly of International Strategic Studies* 3, no. 04 (2017): 499–512.

[6] Stephen Nagy, "Sino-Japanese Reactive Diplomacy as Seen through the Interplay of the Belt Road Initiative (BRI) and the Free and Open Indo-Pacific Vision (FOIP)," *China Report* 57, no. 1 (2021): 7–21.

[7] Ade Priangani and Willya Achmad, "Middle Eastern Geopolitics and the Transformation of Islamic Law: An Analysis of Islamic Politics in Muslim Countries," *Al-Manahij: Jurnal Kajian Hukum Islam*, 2026, 85–98.

[8] Hideaki Shinoda, "The Free and Open Indo-Pacific, the Belt and Road Initiative and BRICS," in *Confronting Theories of Geopolitics: Continental and Anglo-American Traditions* (Springer, 2026), 127–138.

[9] Mohamad Iswan Nusi et al., "Supremasi Kognitif: Pelajaran Dari Kepemimpinan Global Untuk Doktrin Pertahanan Siber Indonesia.," *Jurnal Pendidikan Indonesia* 6, no. 11 (2025).

https://doi.org/10.66325/nusantaralaw.v5i1.296

and regional geopolitical interests[10]. Amidst the escalating strategic rivalry between the United States and China, Indonesia's digital space is vulnerable to influence operations, narrative contestation, and cross-border information dissemination[11]. This vulnerability is exacerbated by the high level of internet penetration and social media usage, which make Indonesia one of the world's largest digital markets but also create a highly fluid, fast-paced, and difficult-to-control information environment.[12]

In addition to external factors, Indonesia's domestic dynamics also increase its vulnerability to cognitive threats[13]. The pluralistic structure of society, the strengthening of political identities, low digital literacy among some groups, and high polarization in electoral political contests create conditions conducive to the spread of information, the radicalization of courage, and the mobilization of public opinion based on emotions and identity sentiments[14]. In such conditions, cognitive threats can no longer be understood simply as communication problems or cyberspace disruptions, but have become a national security issue with the potential to disrupt political stability, social cohesion, the legitimacy of democratic institutions, and the overall resilience of the state.[15] In other words, the digital information space in Indonesia has transformed into a strategic arena where national security is at stake through the struggle for perception, narrative, and control over public opinion[16].

However, traditional security approaches remain inadequate for explaining how the state perceives and responds to cognitive threats.[17] In practice, the securitization of cognitive threats in Indonesia does not occur in a single, centralized manner but rather involves various institutions with overlapping mandates, including the military, intelligence agencies, the cyber agency, the digital regulator, the police, and relevant ministries. Each actor has different interpretations, interests, and operational logics in

[10] Irfan Ardhani, Randy W. Nandyatama, and Rizky Alif Alvian, "Middle Power Legitimation Strategies: The Case of Indonesia and the ASEAN Outlook on the Indo-Pacific," *Australian Journal of International Affairs* 77, no. 4 (2023): 359–379.

[11] Khoirul Amin et al., "Managing Power Rivalry: Indonesia's Perspective and Strategy in Managing Relations with China in the Indo-Pacific," *Dynamics in the Indo-Pacific: From Geopolitics and Geoeconomics Perspectives*, 2024, 73–84.

[12] Edwin Jurriëns and Ross Tapsell, "Challenges and Opportunities of the Digital 'Revolution'in Indonesia," *Digital Indonesia: Connectivity and Divergence* 2020 (2017): 275–288.

[13] Azizah Nur Rahmatika, "Strategi Pertahanan Negara Indonesia Dalam Menghadapi Ancaman Artificial Intelligence," *Peperangan Asimetris (PA)* 8, no. 1 (2022): 84–99.

[14] Alex Young Pedersen, Rikke Toft Nørgaard, and Christian Köppe, "Patterns of Inclusion: Fostering Digital Citizenship through Hybrid Education," *Journal of Educational Technology & Society* 21, no. 1 (2018): 225–236.

[15] Stanisław Kowalkowski, Danuta Kaźmierczak, and Mirosław Laskowski, "Threats to Social Cohesion in Times of New Wars," *Democracy and Security*, 2025, 1–24.

[16] Malwina Anna Siewier, "Resilience as a Strategic Pillar of Cognitive Security," *Humanities and Social Sciences* 32, no. 4 (2025): 169–183.

[17] Elizaveta Gaufman, "Security Threats and Public Perception," *Cham: Springer International Publishing. Doi* 10 (2017): 973–978.

https://doi.org/10.66325/nusantaralaw.v5i1.296

defining threats and determining security responses[18]. As a result, the securitization process is more complex and multidimensional, and it occurs through inter-institutional network interactions rather than simply through vertical relations between the state and society.[19]

Theoretically, this study departs from the Securitization Theory developed by Barry Buzan, Ole Wæver, and the Copenhagen School, which understands security as a performative process in which an issue is constructed as an existential threat through speech acts, thereby legitimizing the implementation of extraordinary measures beyond normal politics[20]. Furthermore, this research draws on Regional Security Complex Theory (RSCT), which explains how security dynamics are shaped by regional interdependence and great-power penetration within a security region.[21] To add a normative dimension, this article also draws on Rita Floyd's Just Securitization Theory, which emphasizes that securitization must be evaluated on the basis of the legitimacy of the threat, the proportionality of the response, and the protection of democratic principles.[22]

However, these approaches still have limitations when applied to contemporary cognitive threats. Classical securitization theory tends to assume the state as a single, coherent, and hierarchical actor and views securitization as a linear process between speech acts, audience acceptance, and policy legitimacy[23]. However, in the context of digital and cognitive threats, security authority is dispersed across multiple institutions that interact, compete, and negotiate in defining the threat. Meanwhile, RSCT focuses more on interstate dynamics and fails to adequately explain how securitization occurs internally within states through domestic institutional networks.[24] On the other hand, the literature on cognitive warfare is still dominated by a Euro-Atlantic perspective and a technological-operational approach, thus paying little attention to how cognitive threats are interpreted and managed in Global South countries like Indonesia[25].

Based on this situation, a significant research gap exists: the absence of a conceptual framework that explains how the securitization of cognitive threats occurs through networks (networked securitization) and involves multiple actors within the

---

[18] Sarwo Edi Wibowo et al., "Securitization of Cyber Threats to the Indonesian Government: A Study of Cyber Defense Strategy," *Global Political Studies Journal* 8, no. 2 (2024): 97–108.

[19] Yandry Kurniawan, *The Politics of Securitization in Democratic Indonesia* (Springer, 2018).

[20] Barry Buzan, Ole Wæver, and Jaap De Wilde, *Security: A New Framework for Analysis* (Lynne Rienner Publishers, 1998).

[21] Barry Buzan and Ole Waever, *Regions and Powers: The Structure of International Security*, vol. 91 (Cambridge University Press, 2003).

[22] Rita Floyd, "Can Securitization Theory Be Used in Normative Analysis? Towards a Just Securitization Theory," *Security Dialogue* 42, nos. 4–5 (2011): 427–439.

[23] Thierry Balzacq, "The Three Faces of Securitization: Political Agency, Audience and Context," *European Journal of International Relations* 11, no. 2 (2005): 171–201.

[24] R. Guy Emerson, "Towards a Process-Orientated Account of the Securitisation Trinity: The Speech Act, the Securitiser and the Audience," *Journal of International Relations and Development* 22, no. 3 (2019): 515–531.

[25] Dagmar Rychnovská, "Securitization and the Power of Threat Framing," *Perspectives: Review of International Affairs*, no. 2 (2014): 9–32.

complex context of domestic security governance. This gap becomes even more significant in the Indonesian context, where digital and information security are not managed by a single institution but rather through plural, intersecting institutional configurations.

Therefore, this article aims to explain how cognitive warfare is securitized in Indonesia through a multi-actor, fragmented, and institutionally network-based process. To explain these dynamics, this article introduces the concept of the National Security Complex (NSC). This framework emphasizes that securitization occurs not only vertically between the state and society but also horizontally through interactions between state institutions with security authority. This concept highlights how coordination, competition, and institutional overlap shape the construction of threats and security responses in the cognitive domain.

Method

This study adopts a qualitative research design grounded in an interpretive and constructivist approach to security analysis. Given that securitization is understood as a socially constructed and discursive process, the study focuses on how threats are articulated, interpreted, and institutionalized rather than treating them as objective and fixed phenomena. The research combines document analysis with interpretive policy analysis to examine how cognitive warfare is constructed as a security issue within Indonesia's defense and governance framework. Primary data sources include official defense documents—such as defense white papers, national defense strategies, doctrinal publications, and policy regulations—as well as publicly available speeches, policy statements, and institutional reports. These materials are complemented by academic literature on cognitive warfare, securitization theory, and Indo-Pacific security dynamics, allowing for triangulation between official discourse and scholarly interpretation.

Analytically, the study employs a multilevel framework that integrates three interconnected layers of analysis. First, the global–regional level examines the broader Indo-Pacific strategic environment, including great power competition, regional security architectures, and the diffusion of cognitive and informational threats. Second, the national–institutional level focuses on the configuration and interaction of domestic actors—such as defense institutions, intelligence agencies, cybersecurity bodies, and regulatory authorities—in shaping the securitization process. Third, the societal–operational level explores how these constructions are translated into policy implementation, public discourse, and societal responses, including issues of audience acceptance and resistance.

Within this framework, the analysis is guided by key concepts derived from securitization theory, including speech acts, referent objects, audience dynamics, and extraordinary measures, as well as their normative evaluation through Just Securitization Theory. In addition, the study incorporates the concept of a *National Security Complex* to capture the horizontal interactions among state institutions, enabling a more refined understanding of how securitization unfolds in fragmented governance environments.
This methodological approach allows the study to capture both the vertical dimension of securitization—linking global, regional, and domestic dynamics—and its horizontal dimension within the state. By combining interpretive analysis with multilevel

structuring, the research provides a comprehensive account of how cognitive warfare is securitized in a democratic Global South context characterized by institutional plurality and a rapidly evolving digital ecosystem.

Result and Discussion

Actors and Institutional Configuration

The securitization of cognitive warfare in Indonesia is characterized by a multi-actor, institutionally distributed configuration, reflecting a departure from the classical model of securitization centered on a singular, authoritative actor. Instead, the Indonesian case demonstrates a layered structure in which authority is dispersed across political, military, intelligence, cyber, and regulatory institutions, each contributing to the construction and operationalization of cognitive threats. At the apex of this configuration are political actors—particularly the President and the Minister of Defense—who function as primary securitizing actors. Through official statements, strategic documents, and policy directives, they articulate cognitive threats as "information warfare," "cyber threats," and a "war of mindset," framing them as risks to national stability, ideological integrity, and political legitimacy. These high-level articulations serve as foundational speech acts that elevate cognitive warfare from a technical or societal issue into a matter of national security.

At the operational level, the Indonesian National Armed Forces (TNI) plays a central role in translating these threat constructions into defense posture, doctrine, and capability development. This includes integrating cyber defense, information operations, and psychological dimensions into broader strategic planning. The expansion of military attention into non-kinetic domains illustrates the growing recognition of the cognitive domain as a legitimate battlespace within contemporary defense thinking. Beyond the military, a range of non-military institutions—including intelligence agencies, national cyber security bodies, and digital regulatory authorities—form the technical and functional backbone of securitization. These actors are responsible for threat detection, data analysis, infrastructure protection, content governance, and policy implementation. Their involvement reflects the non-linear and cross-sectoral nature of cognitive threats, which cannot be addressed solely through traditional defense mechanisms.

Crucially, the interaction among these actors does not form a fully unified or hierarchical system. Instead, it constitutes what this study conceptualizes as a *National Security Complex*—a horizontally structured configuration in which multiple institutions with overlapping mandates, distinct organizational cultures, and varying priorities interact, coordinate, and at times compete in defining and responding to security threats. Within this complex, securitization is not simply the product of top–down authority, but emerges through ongoing processes of negotiation, alignment, and contestation among institutional actors[26]. This institutional plurality has significant implications for the securitization process. On the one hand, it enables a more comprehensive and adaptive response by mobilizing diverse capabilities across sectors. On the other hand, it

[26] Firas Meshhal Abduljabbar et al., "Securitization of Immigration and Refugee Policy in Contemporary Islamic Politics and International Law," *MILRev: Metro Islamic Law Review* 4, no. 1 (2025): 64–98.

introduces coordination challenges, potential policy fragmentation, and inconsistencies in threat framing, which may affect the coherence and effectiveness of securitization. As such, the Indonesian case illustrates that securitization in the cognitive domain is both enabled and constrained by the very institutional complexity that defines contemporary security governance.

Expansion of Referent Objects

The Indonesian case demonstrates a significant expansion of referent objects in the securitization of cognitive warfare, moving beyond the traditional focus on territorial sovereignty toward a more complex configuration of political, informational, and societal domains. This shift reflects a broader transformation in the understanding of security, in which the protection of the state is increasingly intertwined with the protection of cognitive and social structures that sustain it. While territorial integrity and national sovereignty remain foundational referent objects, the analysis shows that securitization discourse in Indonesia increasingly incorporates additional dimensions. These include the protection of democratic processes and political legitimacy, particularly in relation to disinformation and electoral manipulation; the safeguarding of information sovereignty and national cyberspace, in response to concerns over foreign influence and data vulnerability; and the preservation of social cohesion and ideological stability, especially in the face of identity-based polarization, radicalization, and narratives perceived as threatening to the state ideology.

This expansion aligns with the broader framework of sectoral security in securitization theory, in which political and societal security complement traditional military concerns. However, in the context of cognitive warfare, these dimensions are not merely parallel sectors but are deeply interconnected.[27] Threats targeting information flows can simultaneously affect democratic legitimacy, social trust, and national identity, thereby blurring the boundaries between political, societal, and informational security. Importantly, the Indonesian case suggests that referent objects are not only expanding in number but also transforming in nature. Rather than being exclusively material or institutional, referent objects increasingly include intangible elements such as public perception, collective identity, and cognitive resilience. This transformation reflects the logic of cognitive warfare, in which the primary objective is to influence how individuals and societies perceive reality and make decisions.

At the same time, this expansion introduces normative and analytical challenges. The broader and more abstract the referent objects become, the greater the risk of ambiguity in defining threats and justifying policy responses. Concepts such as "social cohesion" or "ideological stability" may be interpreted differently by various actors, creating potential tensions between security objectives and democratic principles[28]. As a

[27] Nita A. Paula, "The Role of the United Nations in Protecting Human Rights in Palestine (The Phase of Post-Al-Aqsa Flood)," *Al-Biruni Journal of Humanities and Social Sciences*, February 17, 2026, 17, https://doi.org/10.64440/BIRUNI/BIR015.

[28] Mahrus Ali, Hamad F. Al-Fahad, and Wasikh Maulana, "Philosophical Foundation, Application, and Controversies of Judicial Pardon in Islamic Criminal Law, Indonesian Penal Code, and the Criminal Justice System of Kuwait," *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 2 (2025): 624–648.

result, the expansion of referent objects not only strengthens the rationale for securitization but also complicates its legitimacy and limits. In this sense, the Indonesian experience illustrates a shift toward what can be described as cognitive–societal security, in which the stability of the state is understood to depend on the integrity of its informational environment, the resilience of its society, and the legitimacy of its political system.

Threat Narratives and Framing

The securitization of cognitive warfare in Indonesia is strongly shaped by the construction of threat narratives that frame emerging risks through a combination of global strategic discourse and domestic socio-political concerns. Rather than relying on a single, coherent terminology, these narratives draw on a range of overlapping concepts, including "information warfare," "cyber warfare," "proxy war," and, most prominently, "war of mindset." This multiplicity of terms reflects both the evolving nature of the threat and the absence of a fully consolidated conceptual framework within policy discourse. At the strategic level, these narratives function as speech acts that elevate cognitive and informational phenomena into matters of national security, by framing disinformation, digital radicalization, and online influence operations as components of warfare, political and defense actors reclassify what might otherwise be treated as social or technological issues into existential threats to the state. In particular, the notion of "war of mindset" emphasizes targeting public perception, ideological orientation, and collective identity, thereby expanding the scope of security beyond the physical and institutional domains.

Importantly, these narratives operate by linking global strategic competition with domestic vulnerabilities. References to great power rivalry—especially in the Indo-Pacific context—are combined with concerns about internal fragmentation, identity-based polarization, and the spread of radical or anti-state ideologies. Through this framing, external threats and internal weaknesses are presented as interconnected, reinforcing the perception that Indonesia is both a target and a battleground within a broader cognitive conflict. At the operational level, the framing of threats is further reinforced by the characterization of information dynamics in the digital ecosystem. The spread of disinformation is often described as systematic, large-scale, and technologically enabled, resembling patterns associated with coordinated influence operations. Concepts such as rapid dissemination, repetition, and multi-platform amplification are used to depict an environment in which false or misleading narratives can shape public opinion at scale. This reinforces the perception of urgency and supports the argument for stronger state intervention.

However, the multiplicity and fluidity of these threat narratives also introduce ambiguity.[29] Different institutions may emphasize different aspects of the threat—ranging from cyber security and infrastructure protection to ideological resilience and social cohesion—resulting in variations in how cognitive warfare is understood and

[29] Yevhen Leheza et al., "Interpretation of Regulatory and Legal Acts in Contemporary Contexts: Foreign Experience, Comparative Perspectives, and Pathways for Regulatory Reform," *Nusantara: Journal of Law Studies* 5, no. 1 (February 2026): 102–122, https://doi.org/10.5281/zenodo.18727992.

addressed. This variability reflects the broader institutional complexity identified in Section 4.1 and underscores the role of narrative construction as a site of both coordination and contestation. In this sense, threat narratives do not merely describe security challenges; they actively shape the boundaries of what is considered a security issue, who is responsible for addressing it, and which responses are deemed legitimate. As such, framing processes are central to the securitization of cognitive warfare, mediating the relationship between abstract global dynamics and concrete domestic policy action.

Institutionalization of Securitization

The findings indicate that the securitization of cognitive warfare in Indonesia has moved beyond episodic or ad hoc responses and has become increasingly institutionalized within the state's security and governance framework. This institutionalization is reflected in the integration of cognitive and informational threats into legal instruments, strategic policy documents, doctrinal frameworks, and organizational structures. At the normative level, securitization is embedded in formal legal and policy frameworks that define the scope of national defense and security. Foundational regulations and defense policies increasingly recognize cyber threats, information manipulation, and psychological operations as components of non-military or hybrid threats. This formal recognition provides the legal basis for expanding the role of state institutions in managing the digital and cognitive domain.

At the strategic level, securitization is further reinforced through defense white papers, national security strategies, and doctrinal publications. These documents incorporate concepts such as information warfare, cyber defense, and asymmetric threats into official threat assessments, thereby institutionalizing cognitive warfare within the broader strategic outlook[30]. The inclusion of these elements signals a shift in defense thinking, treating non-kinetic domains as integral to national security rather than peripheral concerns. At the organizational level, institutionalization is most visible in the development and strengthening of specialized structures dedicated to cyber security, information management, and cognitive threat analysis. These include military and civilian bodies responsible for cyber defense, intelligence coordination, and digital regulation. Their mandates extend beyond technical protection of infrastructure to include monitoring information flows, analyzing narratives, and responding to influence operations, illustrating the operationalization of securitization in the cognitive domain. Importantly, this institutionalization process is not confined to a single agency or sector, but is distributed across multiple institutions, each contributing to different aspects of securitization. This reflects the horizontally structured nature of the National Security Complex conceptualized in this study, in which legal authority, strategic direction, and operational capacity are dispersed across a network of actors. As a result, institutionalization involves not only the creation of new structures, but also the alignment—partial and evolving—of existing institutional mandates with the emerging logic of cognitive security.

[30] Muhammad Alvi Syahrin, "Conflict of Regulation Norms for Handling of Foreign Refugees in Selective Immigration Policies: Critical Law Studies and State Security Approaches," *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat* 20, no. 1 (2020): 67–82.

At the same time, the process remains uneven and incomplete. Variations in institutional priorities, differences in interpretation of cognitive threats, and challenges in inter-agency coordination limit the coherence of securitization. This suggests that institutionalization is not a linear or fully consolidated process, but rather an ongoing negotiation shaped by both structural constraints and political considerations. In this sense, the Indonesian case demonstrates that securitization in the cognitive domain becomes durable not through exceptional emergency measures but through its gradual embedding in routine governance practices, thereby transforming extraordinary concerns into normalized policy domains.

National Security Complex

The findings of this study reveal that the securitization of cognitive warfare in Indonesia operates within what can be conceptualized as the National Security Complex—a horizontally structured configuration of state institutions characterized by interaction, coordination, and competition in the development and management of security threats. This concept captures a critical dimension of securitization often overlooked in the existing literature: the intra-state dynamics that shape how security is defined, prioritized, and operationalized. In contrast to classic securitization models that emphasize relatively unified securitizing actors, the Indonesian case demonstrates that securitization arises from the interaction of multiple institutions with overlapping mandates. Political leaders articulate strategic threat narratives, such as when President Joko Widodo repeatedly asserted that "digital sovereignty must be safeguarded" from polarizing threats. The military then translates this into a defense posture, as seen in the establishment of the Indonesian National Armed Forces Cyber Command (Satsiber TNI) to fortify soldiers and the public from the infiltration of foreign ideologies.

On the other hand, intelligence and cyber agencies such as the State Intelligence Agency (BIN) and the National Cyber and Information Technology Agency (BSSN) focus on detecting and analyzing cyber-psychological attacks. At the same time, the Ministry of Communication and Informatics (Kominfo) regulates digital platforms through content moderation and takedowns. These interactions create a complex network of authorities, rather than a linear chain of command. Within this National Security Complex, securitization is not simply a top-down decision-making process but also an ongoing negotiation among institutional actors. Coordination mechanisms enable policy alignment, as seen in the establishment of the Election Desk by the Coordinating Ministry for Political, Legal, and Security Affairs, which brings together the BSSN, Kominfo, the National Police, and the General Elections Commission (KPU) to address the flood of disinformation leading up to the election. However, differences in institutional priorities and organizational cultures continue to generate contestation. Tensions often arise between the security-oriented approach of law enforcement officials, which emphasizes control, surveillance, and criminalization through the ITE Law, and the governance-oriented approach of civilians, which emphasizes platform regulation, digital literacy, and public engagement. This internal complexity has significant implications for the nature of securitization in the cognitive realm.

On the one hand, the involvement of multiple institutions enhances state capacity; the collaboration between the National Cyber and Information Technology Agency (BSSN) and the Ministry of Communication and Information Technology

(Kominfo) in detecting and blocking radical propaganda sites demonstrates the effectiveness of mobilizing diverse resources. On the other hand, overlapping authority leads to fragmentation. Sectoral egos often slow down policy implementation on the ground, as seen in slow responses to strategic data leaks or hoax labeling that could trigger public legitimacy debates. Thus, securitization within the National Security Complex is inherently uneven, shaped by cooperation and competition among institutional actors. Importantly, the concept of the National Security Complex complements and expands existing theoretical frameworks. While multilevel approaches emphasize vertical interactions between global, regional, and domestic dynamics, the National Security Complex highlights horizontal dimensions within the state itself[31].

Together, these dimensions demonstrate that securitization in the context of cognitive warfare is multilevel and multicentered, requiring an analytical framework that can account for distributed authority and institutional plurality. The Indonesian case demonstrates that understanding contemporary securitization—particularly in the cognitive realm—requires a shift from state-centered and single-actor models to a more nuanced perspective. The state should not be understood as a single, monolithic actor in security, but rather as a complex arena in which security is continuously constructed, negotiated, and contested by various institutions.

Discussion

Networked Securitization

The Indonesian case study demonstrates that securitization in the cognitive realm operates as a networked process involving multiple actors, institutional layers, and socio-technical infrastructure. This finding challenges the classical formulation of securitization theory, which tends to conceptualize security construction as a linear process driven by a central, monolithic securitizing actor targeting a specific, passive audience[32] [33]. In contrast, empirical evidence in Indonesia suggests that securitization is distributed across a network of interacting actors, with each node contributing to the articulation, interpretation, and implementation of security claims. As the findings demonstrate, political leaders serve as the primary initiators of securitization discourse, but their speech acts do not operate in isolation. A dramatic case is seen in the enactment of regulations addressing negative content and misinformation, where the threat narrative from the political elite is immediately amplified in a hybrid manner. This narrative moves from official statements by state officials, interpreted as Cyber and Intelligence operations by institutions such as the National Cyber and Information

[31] Taufiq Shobri et al., "Legal Framework for Addressing Cybercrime Threats in Strengthening Indonesia's National Defense and Security," *Trunojoyo Law Review* 8, no. 2 (2026).

[32] Beny Abukhaer Tatara, Suhirwan Suhirwan, and Mochammad Afifuddin, "The Active Defense Strategy of the National Narcotics Board of the Republic of Indonesia in Facing Asymmetric Warfare," *International Journal of Advances in Social and Economics* 4, no. 3 (2022): 84–89.

[33] Shuang Wang et al., "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector," *Computers & Security* 147 (2024): 104051.

Agency (BSSN) and the State Intelligence Agency (BIN), to tactical policies of access cuts by the Ministry of Communication and Informatics.[34]

However, this network extends far beyond formal state institutions to encompass socio-technical elements such as digital platforms (X, Meta, TikTok) and information infrastructure. In Indonesia, the securitization of this network is driven primarily by an ecosystem of non-state actors, including political buzzer networks, pro-government influencers, and digital volunteers (cyber armies). When the government designates an issue as a "cognitive threat" or a "hoax that threatens stability," this network of non-state actors uses the platform's algorithmic system, through trending topic manipulation and hashtag amplification, to dominate the digital public space. This distributed configuration emphasizes that authority in cognitive securitization is no longer centralized but rather relational, emerging from the dynamic interaction among state legal institutions, paid digital agents, and the platform's technological architecture.

The character of this network fundamentally changes the role of the audience. Rather than acting as passive recipients of state security narratives, audiences in the Indonesian context are highly fragmented, diverse, and actively engaged in interpreting, replicating, or even challenging them. This fragmentation is evident in Indonesia's persistent digital polarization. For example, when the state launches a securitization narrative against opposition movements or public criticism by labeling them as "unity-destroying disinformation" or "radicalism," audiences do not respond uniformly. Pro-government segments of society will reinforce these claims by spreading counter-content, while segments of civil society and netizen communities (such as the spontaneous counter-narrative movement in X) engage in open resistance by exposing government data manipulation. Consequently, securitization in the cognitive domain is often partial, uneven, and experiences legitimacy leaks across various segments of society[35].

Theoretically, the concept of network securitization complements the notion of the National Security Complex developed in this study. While the National Security Complex captures horizontal institutional dynamics and the struggle for influence within the state bureaucracy, network securitization expands its analysis outward, encompassing the fluid interactions between state actors, civil society actors, the technology industry, and the algorithmic infrastructure of digital platforms. Together, these two concepts demonstrate that securitization in the contemporary cognitive realm is multi-centered and multi-layered. In this context, the Indonesian case provides strong empirical support for rethinking securitization no longer as an absolute state prerogative, but as a distributed security governance process. In the digital era, power is no longer exercised solely through centralized, top-down command and control, but rather through the capacity to control, manipulate, and navigate networks of actors and technological infrastructures that condition public cognition.

---

[34] Rahmatika, "Strategi Pertahanan Negara Indonesia Dalam Menghadapi Ancaman Artificial Intelligence."

[35] Arief Prayitno and Rudiyanto Rudiyanto, "Defending the Nation in the Cyber Era: Indonesia's Response to Non Military Security Threats," *Enrichment: Journal of Multidisciplinary Research and Development* 3, no. 9 (2025): 3520–3532.

Cognitive Turn in Security

Security is increasingly oriented toward cognitive dimensions, emphasizing perception, narrative construction, and psychological influence as central arenas of contemporary conflict. This shift reflects a broader transformation in the character of warfare, where the primary objective is no longer limited to the control of territory or the destruction of physical assets, but extends to shaping how individuals and societies perceive reality and make decisions[36]. This *cognitive turn* in security aligns closely with the literature on fifth-generation warfare (5GW), hybrid warfare, and gray-zone conflict, all of which highlight the growing importance of non-kinetic strategies that operate below the threshold of conventional war. In this context, information manipulation, disinformation campaigns, and narrative competition become key instruments of power, often deployed through digital platforms and algorithmically mediated environments. As a result, the battlespace expands from physical and institutional domains into the cognitive sphere, where meaning, belief, and identity are contested[37].

The findings of this study demonstrate that this transformation is clearly reflected in the Indonesian context. Threat narratives articulated by political leaders and institutional actors increasingly employ concepts such as "information warfare," "cyber warfare," and particularly "war of mindset," indicating an explicit recognition that the primary target of contemporary conflict is the cognitive domain of society. These narratives are further reinforced by policy frameworks, doctrinal developments, and institutional arrangements that integrate cyber security, information operations, and social resilience into the broader architecture of national defense.

At the same time, the expansion of referent objects—from territorial sovereignty to include democracy, information sovereignty, social cohesion, and ideological stability—illustrates how security concerns are increasingly tied to the integrity of cognitive and societal systems. In this sense, the protection of the state is inseparable from the protection of collective perception, public trust, and the informational environment in which political and social life unfolds. However, the cognitive turn also introduces significant complexity into the securitization process. Unlike traditional threats, which are relatively tangible and attributable, cognitive threats are diffuse, ambiguous, and often embedded in everyday communication practices. They operate through decentralized networks, involve both state and non-state actors, and are mediated by technological systems that are not fully controlled by the state. Consequently, the boundaries between threat and normal political contestation become blurred, making it more difficult to define what constitutes an existential threat and what constitutes legitimate expression or dissent. This ambiguity has important implications for securitization. While the cognitive domain clearly represents a critical frontier of contemporary security, its inherently fluid and contested nature challenges states' ability to securitize it coherently and fully. As the next section will argue, these characteristics

[36] Felix Ciută, "Narratives of Security: Strategy and Identity in the European Context," in *Discursive Constructions of Identity in European Politics* (Springer, 2007), 190–207.

[37] Hilkka Grahn and Toni Taipalus, "Defining Comprehensive Cognitive Security in the Digital Era: Literature Review and Concept Analysis," *Journal of Information Warfare*, no. 2 (2025).

place structural limits on the securitization of cognitive warfare, raising questions about the extent to which such processes can be effectively and normatively sustained.

National Security Complex as a Theoretical Contribution

The concept of a *National Security Complex* provides a new analytical lens for understanding securitization as a multi-centered and internally contested process within the state. While classical securitization theory emphasizes the role of a primary securitizing actor—typically political elites—articulating existential threats to a relatively unified audience, the findings of this study demonstrate that such a model is insufficient to explain the dynamics of securitization in contemporary, institutionally complex democracies. In the Indonesian case, securitization does not emanate from a single authoritative center but rather unfolds through the interaction of multiple state institutions, including political leadership, defense establishments, intelligence agencies, cybersecurity bodies, law enforcement, and regulatory authorities. These actors do not merely implement a unified security narrative; they actively participate in defining, interpreting, and operationalizing threats, often from different institutional mandates, epistemic frameworks, and operational priorities.

This configuration produces what can be conceptualized as a *National Security Complex*: a structured yet dynamic field of interaction in which state institutions are simultaneously engaged in coordination, competition, and negotiation over the meaning of security and the appropriate forms of response. Within this complex, securitization becomes a process that is not only multilevel (linking global, regional, and domestic dynamics) but also multi-centered at the domestic level, reflecting the fragmentation and pluralization of authority in modern governance systems.

The empirical findings show that institutions such as the Ministry of Defense, the military, intelligence agencies, cyber security authorities, and communication regulators each contribute distinct perspectives to the construction of cognitive threats. For instance, while defense institutions tend to frame cognitive warfare in terms of national resilience and strategic competition, regulatory bodies often approach it through the lens of information governance and platform control, and law enforcement agencies emphasize legal enforcement and public order. These differing perspectives generate both complementarities and tensions, shaping the trajectory of securitization in ways that a linear or actor-centric model cannot capture. Importantly, the National Security Complex also incorporates the role of non-state and socio-technical actors, including epistemic communities, civil society organizations, and digital platforms. Although not formally part of the state, these actors influence how threats are understood, contested, and legitimized, thereby contributing to the broader ecosystem in which securitization takes place. This further reinforces the argument that securitization in the cognitive domain operates through a distributed, relational structure rather than a centralized hierarchy.

As a theoretical contribution, the concept of a National Security Complex extends securitization theory in two keyways. First, it introduces an intra-state dimension that complements the inter-state focus of frameworks such as the Regional Security Complex Theory (RSCT), thereby capturing how internal institutional dynamics shape the articulation and implementation of security policies. Second, it provides a bridge between securitization theory and contemporary governance approaches that emphasize

networked, multi-actor, and socio-technical configurations of power. By conceptualizing securitization as a process embedded within a National Security Complex, this study highlights that the production of security is not merely a matter of political declaration, but a negotiated outcome of institutional interactions within the state. This perspective is particularly relevant for understanding cognitive warfare, where ambiguity, technological mediation, and societal embeddedness amplify the need for coordination while simultaneously increasing the potential for fragmentation and contestation. Ultimately, the National Security Complex framework offers a more nuanced understanding of how securitization operates in the Global South, where institutional pluralism, evolving governance structures, and socio-political diversity create conditions under which security is continuously constructed, contested, and redefined.

Conclusion

This article has demonstrated that the securitization of cognitive warfare in Indonesia cannot be adequately understood through conventional, state-centric models of security. Instead, it is best conceptualized as a networked, institutionally distributed process shaped by the interactions among multiple actors, domains, and levels of governance. By tracing how threat narratives are constructed, institutionalized, and operationalized, the study shows that securitization in the cognitive domain extends beyond traditional military and territorial concerns to encompass perception, information flows, and societal resilience. A central contribution of this article is the introduction of the National Security Complex as a conceptual framework for capturing the intra-state dimension of securitization. This framework highlights how security is produced not by a single authoritative actor, but through dynamic interactions among political leaders, defense institutions, intelligence agencies, cyber security bodies, regulatory authorities, and socio-technical actors. In doing so, it reveals that securitization is not only multilevel—linking global, regional, and domestic contexts—but also multi-centered within the state, reflecting institutional pluralism and contested authority in contemporary governance. The findings further demonstrate that the rise of cognitive warfare marks a broader transformation in the character of conflict, where the primary battlespace shifts toward the cognitive and informational domains. This shift challenges existing theoretical assumptions by blurring the boundaries between war and peace, security and politics, and state authority and societal processes. As a result, securitization becomes more complex, less linear, and increasingly embedded in digital and social infrastructures that are only partially under state control.

Importantly, the Indonesian case illustrates that, while the securitization of cognitive threats is empirically grounded and institutionally evolving, it also faces structural and normative constraints. The diffuse, ambiguous, and socially embedded nature of cognitive threats complicates the identification of clear referent objects and proportional responses, raising the risk of over-securitization and the erosion of civil liberties. This underscores the need to balance security imperatives with democratic accountability and the protection of fundamental rights. More broadly, this study suggests that securitization theory must evolve to account for three interrelated transformations: the cognitive turn in security, the networked and socio-technical nature of contemporary threats, and the internal fragmentation of state authority captured by

the concept of a National Security Complex. In this sense, the Global South—far from being a peripheral case—emerges as a critical site for theoretical innovation, where the interaction between technological disruption, institutional diversity, and democratic contestation generates new forms of security governance. Future research should further explore how these dynamics unfold across different political systems and regional contexts, as well as how normative frameworks can be refined to guide the securitization of cognitive threats in ways that remain both effective and just. Ultimately, understanding cognitive warfare requires not only new policy responses but also a rethinking of the conceptual foundations of security itself.

Acknowledgement

The authors would like to express their sincere gratitude to the Dean of the Faculty of Social and Political Sciences, Universitas Padjadjaran, for the institutional support and academic encouragement provided throughout the completion of this research. The authors also appreciate the conducive academic environment and administrative assistance that contributed significantly to the successful conduct of this study.

Author Contributions Statement

Alzaki Alzaki contributed to the conceptualization of the study, data curation, investigation process, methodology development, and preparation of the original draft manuscript. Arfin Sudirman was responsible for supervision, validation, formal analysis, and reviewing and editing the manuscript critically. R. Widya Setiabudi Sumadinata contributed to the development of the theoretical framework, provision of resources, project administration, and critical revision of the manuscript. Wawan Budi Darmawan and Ola Madallah aljaafreh contributed to data analysis, interpretation of research findings, visualization, and finalization of the manuscript. All authors have read and approved the final version of the manuscript and agreed to be accountable for all aspects of the work.

AI Usage Statement

The authors declare that artificial intelligence (AI)-assisted tools were used solely to support language improvement, grammar checking, and manuscript editing during the preparation of this article. All conceptual development, data analysis, interpretation of findings, and conclusions remain the full responsibility of the authors. The authors have carefully reviewed and validated all content to ensure its accuracy, originality, and compliance with academic integrity and publication ethics.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article. The research was conducted independently without any financial, institutional, commercial, or personal relationships that could influence the objectivity, interpretation, or presentation of the findings presented in this study.

References

A. Paula, Nita. "The Role of the United Nations in Protecting Human Rights in Palestine (The Phase of Post-Al-Aqsa Flood)." *Al-Biruni Journal of Humanities and Social Sciences*, February 17, 2026, 17. https://doi.org/10.64440/BIRUNI/BIR015.

Abduljabbar, Firas Meshhal, Saad Abdulhameed Shalev, Rami Salih, Oudha Yousif Salman Al-Musawi, and Yurii Khlaponin. "Securitization of Immigration and Refugee Policy in Contemporary Islamic Politics and International Law." *MILRev: Metro Islamic Law Review* 4, no. 1 (2025): 64–98.

Adler, Emanuel. "Cognitive Evolution: A Dynamic Approach for the Study of International Relations and Their Progress." *Progress in Postwar International Relations* 43 (1991): 56.

Ali, Mahrus, Hamad F. Al-Fahad, and Wasikh Maulana. "Philosophical Foundation, Application, and Controversies of Judicial Pardon in Islamic Criminal Law, Indonesian Penal Code, and the Criminal Justice System of Kuwait." *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 2 (2025): 624–648.

Amin, Khoirul, Devy Indah Paramitha, Mohamad Dziqie Aulia Al Farauqi, and Anita Shalehah. "Managing Power Rivalry: Indonesia's Perspective and Strategy in Managing Relations with China in the Indo-Pacific." *Dynamics in the Indo-Pacific: From Geopolitics and Geoeconomics Perspectives*, 2024, 73–84.

Ardhani, Irfan, Randy W. Nandyatama, and Rizky Alif Alvian. "Middle Power Legitimation Strategies: The Case of Indonesia and the ASEAN Outlook on the Indo-Pacific." *Australian Journal of International Affairs* 77, no. 4 (2023): 359–379.

Balzacq, Thierry. "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11, no. 2 (2005): 171–201.

Buzan, Barry. "New Patterns of Global Security in the Twenty-First Century." *International Affairs (Royal Institute of International Affairs 1944-)*, 1991, 431–451.

Buzan, Barry, and Ole Waever. *Regions and Powers: The Structure of International Security*. Vol. 91. Cambridge University Press, 2003.

Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998.

Ciută, Felix. "Narratives of Security: Strategy and Identity in the European Context." In *Discursive Constructions of Identity in European Politics*, 190–207. Springer, 2007.

Emerson, R. Guy. "Towards a Process-Orientated Account of the Securitisation Trinity: The Speech Act, the Securitiser and the Audience." *Journal of International Relations and Development* 22, no. 3 (2019): 515–531.

Floyd, Rita. "Can Securitization Theory Be Used in Normative Analysis? Towards a Just Securitization Theory." *Security Dialogue* 42, nos. 4–5 (2011): 427–39.

Gaufman, Elizaveta. "Security Threats and Public Perception." *Cham: Springer International Publishing. Doi* 10 (2017): 973–78.

Grahn, Hilkka, and Toni Taipalus. "Defining Comprehensive Cognitive Security in the Digital Era: Literature Review and Concept Analysis." *Journal of Information Warfare*, no. 2 (2025).

Jurriëns, Edwin, and Ross Tapsell. "Challenges and Opportunities of the Digital 'Revolution'in Indonesia." *Digital Indonesia: Connectivity and Divergence* 2020 (2017): 275–88.

Kefeli, Igor F., Roman S. Vykhodets, and Olga V Plebanek. "Updating Cognitive Security in a Global Dimension." *Journal of Globalization Studies* 16, no. 1 (2025): 39–46.

Kowalkowski, Stanisław, Danuta Kaźmierczak, and Mirosław Laskowski. "Threats to Social Cohesion in Times of New Wars." *Democracy and Security*, 2025, 1–24.

Krause, Keith, and Oliver Jütersonke. "Peace, Security and Development in Post-Conflict Environments." *Security Dialogue* 36, no. 4 (2005): 447–62.

Kurniawan, Yandry. *The Politics of Securitization in Democratic Indonesia*. Springer, 2018.

Leheza, Yevhen, Oleksandr Kurakin, Olha Shapovalova, Kateryna Sokh, and Artur Makarov. "Interpretation of Regulatory and Legal Acts in Contemporary Contexts: Foreign Experience, Comparative Perspectives, and Pathways for Regulatory Reform." *Nusantara: Journal of Law Studies* 5, no. 1 (February 2026): 102–22. https://doi.org/10.5281/zenodo.18727992.

Nagy, Stephen. "Sino-Japanese Reactive Diplomacy as Seen through the Interplay of the Belt Road Initiative (BRI) and the Free and Open Indo-Pacific Vision (FOIP)." *China Report* 57, no. 1 (2021): 7–21.

Nusi, Mohamad Iswan, David Mulyadi Cokabo, Tarsisius Susilo, Teguh Heri Susanto, and Rudi Firmansyah. "Supremasi Kognitif: Pelajaran Dari Kepemimpinan Global Untuk Doktrin Pertahanan Siber Indonesia." *Jurnal Pendidikan Indonesia* 6, no. 11 (2025).

Pedersen, Alex Young, Rikke Toft Nørgaard, and Christian Köppe. "Patterns of Inclusion: Fostering Digital Citizenship through Hybrid Education." *Journal of Educational Technology & Society* 21, no. 1 (2018): 225–236.

Prayitno, Arief, and Rudiyanto Rudiyanto. "Defending the Nation in the Cyber Era: Indonesia's Response to Non Military Security Threats." *Enrichment: Journal of Multidisciplinary Research and Development* 3, no. 9 (2025): 3520–3532.

Priangani, Ade, and Willya Achmad. "Middle Eastern Geopolitics and the Transformation of Islamic Law: An Analysis of Islamic Politics in Muslim Countries." *Al-Manahij: Jurnal Kajian Hukum Islam*, 2026, 85–98.

Rahmatika, Azizah Nur. "Strategi Pertahanan Negara Indonesia Dalam Menghadapi Ancaman Artificial Intelligence." *Peperangan Asimetris (PA)* 8, no. 1 (2022): 84–99.

Rychnovská, Dagmar. "Securitization and the Power of Threat Framing." *Perspectives: Review of International Affairs*, no. 2 (2014): 9–32.

Saeed, Muhammad. "From the Asia-Pacific to the Indo-Pacific: Expanding Sino-US Strategic Competition." *China Quarterly of International Strategic Studies* 3, no. 04 (2017): 499–512.

Shinoda, Hideaki. "The Free and Open Indo-Pacific, the Belt and Road Initiative and BRICS." In *Confronting Theories of Geopolitics: Continental and Anglo-American Traditions*, 127–38. Springer, 2026.

Shobri, Taufiq, Purnomo Yusgiantoro, Djoko Andreas Navalino, and Sutanto Sutanto. "Legal Framework for Addressing Cybercrime Threats in Strengthening Indonesia's National Defense and Security." *Trunojoyo Law Review* 8, no. 2 (2026).

Siewier, Malwina Anna. "Resilience as a Strategic Pillar of Cognitive Security." *Humanities and Social Sciences* 32, no. 4 (2025): 169–83.

Syahrin, Muhammad Alvi. "Conflict of Regulation Norms for Handling of Foreign Refugees in Selective Immigration Policies: Critical Law Studies and State Security Approaches." *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat* 20, no. 1 (2020): 67–82.

Tatara, Beny Abukhaer, Suhirwan Suhirwan, and Mochammad Afifuddin. "The Active Defense Strategy of the National Narcotics Board of the Republic of Indonesia in Facing Asymmetric Warfare." *International Journal of Advances in Social and Economics* 4, no. 3 (2022): 84–89.

Wang, Shuang, Muhammad Asif, Muhammad Farrukh Shahzad, and Muhammad Ashfaq. "Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector." *Computers & Security* 147 (2024): 104051.

Wibowo, Sarwo Edi, Ari Hartono, Hendri Kiswanto, Jafirman Torang Avery Louerens, and Henike Primawanti. "Securitization of Cyber Threats to the Indonesian Government: A Study of Cyber Defense Strategy." *Global Political Studies Journal* 8, no. 2 (2024): 97–108.

https://doi.org/10.66325/nusantaralaw.v5i1.296