Journal of Business, Social and Technology
Volume 7, Issue 3, 1-14
e_ISSN: 2807-6362
https://bustechno.polteksci.ac.id/index.php/jbt/index
DOI: doi.org/10.59261/jbt.v7i3.646

Critical Analysis of Indonesia's Cybersecuritization Discourse: Deconstructing the Identification of Securitizing Actors

***Kamil Ghiffary A**
UPN Veteran Jakarta, Indonesia

Hartanto
UPN Veteran Jakarta, Indonesia

Ivandra Solihin
UPN Veteran Jakarta, Indonesia

***Corresponding author:**
Kamil Ghiffary A, UPN Veteran Jakarta, Indonesia.
✉ghiffaryabdurrahman@upnvj.ac.id

Article Info:

Article history:
Received: April 25, 2026
Revised: May 29, 2026
Accepted: June 09, 2026

Keywords:
Critical Literature Review; Cybersecuritization; Indonesia Cybersecurity; Myriam Dunn Cavelty; Securitization Theory; Speech Act

Abstract

Background: The discussion regarding *Securitization Theory* in academic literature about state reactions to digital threats is growing alongside the development of Indonesia's digital threat landscape. Yet, this study highlights a methodological shortcoming: existing literature often derives from overly simplistic theories, treating securitization as a mere contextual phenomenon rather than assuming it as an active constructivist frame.

Objective: By juxtaposing the structural grammar of the *Copenhagen School* theory with Myriam Dunn Cavelty's concept of *cybersecuritization*, this paper critically engages with recent literature on Indonesia's cybersecuritization.

Methods: Using a qualitative-descriptive *Critical Literature Review*, this study employs the existing academic discourse as its primary data source, addressing the need to deconstruct two fundamental theoretical building blocks of the concept of securitization—securitizing actors and speech acts.

Results: The findings indicate that previous research misapplied the concept of the *speech act*, taking routine political (locutionary) rhetoric literally and failing to deconstruct its illocutionary intent, contextual purpose, or sequentiality. Moreover, the literature remains grounded in traditional, realist models of "existential threats" and tends to overlook technocratic, risk-management practices and non-traditional actors that characterize modern cybersecurity governance. In conclusion, this study advocates for a methodological recommitment, recommending that researchers combine language-specific indicators with features unique to the digital environment.

Conclusion: Acknowledging its focused scope on actors and speech acts, this paper recommends that future research explore the remaining components of the cybersecuritization framework to achieve a complete and dynamic understanding of Indonesia's digital security institutionalization.

To cite this article: Ghiffary, K. A., Hartanto, H., & Solihin, I. (2026). Critical analysis of Indonesia's cybersecuritization discourse: Deconstructing the identification of securitizing actors. Journal of Business, Social and Technology, 7(3), 1–14. https://doi.org/10.59261/jbt.v7i3.646

INTRODUCTION

Golden Generation Indonesia 2045 is a political narrative that was continuously utilized under the presidential administration of Joko Widodo (2019–2024) and continued by the newly elected president Prabowo Subianto as a symbol of their massive commitment to Indonesian youth and its next generation. Under their leadership, this commitment translated into numerous state-level initiatives and policy implementations, one of which is Indonesia Digital 2045: a 'national blueprint' for Indonesia's cyber infrastructure development over the next two decades.

Apart from this national roadmap, the concept of State's Digital Sovereignty or Kedaulatan Data has also been extensively domesticated and discussed in numerous ministerial and governmental meetings in Indonesia since 2018: (1) an act of possessing full rights over a digital product and content in cyberspace (Reindl, 1998); (2) an act of preserving, protecting, and supporting any digital product and substance originating from Indonesia (Fauzi et al., 2024); (3) an act of preserving the digital domain as a source of unity and prosperity for the people (Taylor, 2022); (4) an act of transforming cyberspace to align with Indonesia's national interests (Febriawan & Marisa, 2024). The rhetoric surrounding Kedaulatan Digital remains open to interpretation, but its repeated emphasis in governmental discourse demonstrates Indonesia's determination in the global cyber domain.

However, things seem to be moving in the opposite direction for Indonesia. In 2024–2025 alone, the country experienced a triple threat of cyber incidents: (1) BSI's ransomware incident; (2) the national shock of the PDNS 2.0 ransomware attack; and (3) additional BSI ransomware incidents. Indonesia faced a critical governance failure following the incident at Pusat Data Nasional Sementara (PDNS) in 2024, symbolizing a massive cybersecurity crisis and unpreparedness—a situation analogous to 9/11, where cybersecurity had not yet evolved into global security norms since Estonia's 'Bronze Soldier' cyber crisis in 2007–2008.

Official reports disclosed by Indonesia's key stakeholders at the time indicate that Mr. Budi Arie Setiadi, then Minister of Information and Communication (Kemkominfo), stated that the critical cyber incidents targeting governmental digital infrastructure were initiated by Brain Cipher, a Russian-based variant of LockBit 3.0 ransomware. This ransomware encrypts system access, locking down operations until a ransom is paid; the attackers demanded USD 8 million. A spokesperson from Badan Siber dan Sandi Negara (BSSN) or National Cyber and Crypto Agency reported that active sabotage occurred three days prior to the incidents by an unknown actor, who intentionally disabled the system defense mechanism, namely Windows Defender.

There are no formal indictments regarding the attacker's intent beyond the apparent financial motive, but the incidents caused a 100-hour halt in the national migration system, provoking international outrage. Every major transportation hub in Indonesia (Jakarta's CGK, Bali's DPS, Surabaya's JND) and major ports were forced to operate using manual documentation. Up to 286 governmental services across 56 ministerial establishments were affected, with potential national-scale economic losses estimated at USD 375 million. In the following days, numerous governmental responses were issued despite the system not being fully restored: (1) calling all governmental institutions to audit, evaluate, and back up remaining accessible data to formulate solutions; (2) anticipating further similar national-scale incidents. The situation deescalated after the hackers disclosed the PDNS encryption key via the dark web, following Indonesia's refusal to pay the ransom—a symbolic loss in the public eye. Public expectations for enhanced national cyber resilience are justified, as a similar case had occurred previously: LockBit 3.0 ransomware attacked Bank Syariah Indonesia (BSI) in 2023. This indicates a systemic loop of 'bureaucratic amnesia.'

The empirical point is clear: the government has repeatedly lost ground against cyber attacks over the last five years. One might argue that Indonesia has struggled to respond effectively against unfamiliar threats, but a fundamental question remains: has Indonesia exhausted its political capacity to thwart and mitigate national-scale cyberattacks. Have adequate measures been taken to safeguard national digital infrastructure. If the process of securitization is part of the solution, has Indonesia effectively securitized its digital domain. What has been the trajectory of cybersecuritization studies in Indonesia over the past five years.

To address these questions, a transcendence from empirical evidence to a more objective, methodologically grounded analysis is necessary—an emphasis on process rather than outcome. Literature sharing similar concerns regarding Indonesia's effort to securitize its cyber domain has been identified and reviewed for clarification. Research Objectives: This paper pursues three explicit objectives: (1) to critically assess how securitizing actors are identified in existing Indonesian cybersecuritization literature; (2) to evaluate the methodological rigor applied in analyzing speech acts across reviewed studies; and (3) to apply Dunn Cavelty's cybersecuritization framework as a corrective lens to map discursive gaps. The broader implications of this research serve practitioners and policymakers in Indonesia, particularly those

involved in BSSN's institutional development and national cyber policy formulation, by highlighting how theoretical clarity can improve policy coherence in national cybersecurity governance.

Literature Review

Using the nuance of 'the dynamics of cybersecuritization studies in Indonesia' as the general framing for this literature review—which emphasizes research analyzing recent discourse and studies about Indonesia's dynamic development in cybersecuritization—there are no exact past studies that explore the topic. Instead, the term 'cybersecurity in Indonesia', which frames 'cyber-attack' and 'cyberthreat' in past literature, leans more towards: (1) the analysis of Securitization Theory (Aji, 2025; Azis & Azhari, 2025; Lee, 2020; Putri, 2023; Wibowo et al., 2024). Other perspectives, namely (2) manunggalism and geometripolitization in cyberspace (Arianto & Anggraini, 2025); (3) the role of the state in cybersecurity (Rai et al., 2022); (4) cyberactivism (Juned et al., 2024); (5) cybersecuritization through institutionalization efforts (Aji et al., 2025). Apart from these perspectives, the research methods in these studies generally adopt Creswell and Creswell's (2018) qualitative, descriptive-based framework.

Using a taxonomy-based model and controlling for the variables or objects of analysis in this literature review, there are variations in the domains of 'cyberthreat' discussed. Within the primary category of studies employing Securitization Theory as the main analytical lens, the problems examined as case studies vary: (1) online hoaxes; (2) harmful online content; and (3) illegal online gambling sites. In a broader perception of cyber threats, Wibowo (2024) and Aji (2025) agree that securitization efforts addressing looming threats in Indonesia's cyberspace require institutionalization—Wibowo (2024) emphasizes the Ministry of Defense, whereas Aji focuses on strengthening the National Cyber and Crypto Agency (BSSN) of Indonesia.

As also suggested in the initial categorization, the Copenhagen School approach to Securitization Theory has been the mainstream theoretical approach, serving as an analytical lens in past literature—a more conservative, traditional approach to exploring securitization in cyberspace. In their respective works, Lee (2020) examined how online hoaxes and fake information during the 2019 Indonesian Presidential Elections could be perceived as national threats; Putri (2023) raised concerns regarding an 'overly securitized' freedom of speech and online content; Azis (2025) shifted the focus from internal issues to transnational, multilateral problems, namely syndicates of illegal and illegitimate online gambling sites in Southeast Asia as potential national threats. With a more progressive approach still inspired by traditional securitization, Aji (2025) proposed a multi-track theoretical framework by employing Cyber-sovereignty Theory, Qiao-Franco (2024) alongside Cybersecurity Politics Theory (Dunn Cavelty & Wenger, 2020).

Several key points emerge from this literature review. First, there are 'dynamics of politics' that may occur during securitization. Alongside this, a clear definition of 'de-securitization' is critical to understanding Securitization Theory: emphasizing the reduction of 'extraordinary measures' in a security response back to its original level. Few past studies incorporate these two concepts, highlighting a research gap that warrants reassessment. Second, the gap lies in the constructivist approach, which posits that security is a subjective construction established by securitizing actors. Security is a matter of declaration; however, this paper does not treat every 'declaration' as a 'speech act'.

According to Kurniawan (2018), there are three sequential components of a 'speech act': (1) locutionary—declaring something; (2) illocutionary—implying something; and (3) perlocutionary—combining action and speech (Vuori, 2008). Further distinguishes multiple forms: (1) assertive; (2) directive; (3) commissive; (4) expressive; and (5) declarative speech acts. Applying this understanding to prior literature reveals that many articles neglect: (1) deconstructing textual and verbal documents and (2) examining the relationship between threat declarations and the 'audience', treating all statements as uniform 'speech acts' by securitizing actors—a gap warranting further exploration. Third, newer theoretical frameworks contextualizing Securitization Theory in cybersecurity exist, notably Dunn Cavelty's Cybersecuritization Theory, which advances key variables: (1) identification of 'possible risks' rather than immediate threats (Cavelty, 2012); (2) emphasis on 'technocratization' over 'speech

acts' (Dunn Cavelty, 2013); (3) institutionalization as the manifestation of 'extraordinary measures' (Cavelty & Egloff, 2019); and (4) more inclusive 'securitizing actors' (Dunn Cavelty, 2013). A detailed discussion follows in the next chapter.

Synthesizing these gaps highlights an underlying issue: Indonesian cybersecurity scholarship is theoretically reductive. Past literature often provides a naïve reading, treating every state declaration as a generalized 'speech act' without accounting for technocratic realities in cyberspace. Consequently, this paper aims for a critical re-analysis of literature on the securitization of Indonesia's cyber domain, through systematic deconstruction of actor identification, types of speech acts, and application of Dunn Cavelty's framework to accurately map the evolving discourse.

Theoretical Framework

This study is theoretically framed by the foundation of Securitization Theory, building upon ideas originally developed by the Copenhagen School (Buzan et al., 1998). Security, in its traditional understanding, is not an actual material reality but a socially constructed state of affairs. According to Buzan (1998) by means of a speech act, an issue is justifiably transformed into a security threat. This requires the establishment of a securitizing actor (usually some state elite), who calls an existential threat to a referent object (most commonly state sovereignty or national survival) (Buzan et al., 1998). This threat representation becomes accepted by the relevant audience, legitimizing the actor to impose extraordinary measures that violate normal political means (such as mobilization of the national military or the suspension of civil liberties). Four important components of securitization are identified in the definition, as summarized by (Kurniawan, 2018).

Nevertheless, despite the Copenhagen School providing the fundamental grammar of securitization, utilizing its core framework to comprehend processes occurring in digital spaces is analytically problematic. Cyberspace is an unconventional security domain where the formality of state borders, visible military infrastructures, and immediate physical violence do not exist. Thus, to investigate the securitization of the digital domain, this research draws on a framework for cybersecuritization established by Myriam Dunn Cavelty, who adapts conventional logic from Copenhagen School formalisms into terms that more accurately represent both technical and political realities in cyberspace. Traditional securitization relies heavily on rhetoric of an absolute existential threat that must be eliminated almost immediately. Cavelty (2013) notes that although political rhetoric occasionally employs cyber-doom narratives, such as the notion of a Cyber Pearl Harbor, cybersecuritization in operational and discursive practice is heavily reliant on risk and vulnerability vocabulary. Due to the ubiquitous, omnipresent, and constantly evolving nature of cyber threats—such as malware, espionage, and data breaches—achieving absolute security is inherently unachievable. Consequently, what is at stake in cyberspace shifts from the defeat of a single existential foe (traditional threat model) to risk management and systemic resilience (Dunn Cavelty, 2013).

This change in the content of threats also affects the way in which the speech act occurs and, possibly more importantly, who delivers it. Traditional securitization is based on pronounced, public political speech acts. In sharp contrast, cybersecuritization is technologized to an extreme degree (Hansen & Nissenbaum, 2009). Because cyberspace is inherently complex, Cavelty (2013) refers to the actual construction of the threat primarily as a techno-bureaucratic matter, driven by technical experts, bureaucratic agencies, or cybersecurity professionals rather than securitizing actors as defined by Buzan, namely politicians and governmental institutions. Consequently, what should have been the communicative act of public political discourse is translated into specialist language, risk assessment reports, and government policy briefs. Specialized knowledge, rather than political power, establishes the veracity of the threat. Moreover, as cyberspace is largely a private domain, the actors making these securitizing claims are often non-state actors. According to Cavelty (2019), private tech companies, internet service providers, and cybersecurity firms are major securitizing actors, as they possess the technical capability to identify and articulate low-profile threats.

This situation blurs the line between national security and private interests, since what is being protected (the referent objects of security, which can range from banking systems to

telecommunications networks to private citizen data) is largely beyond direct state control. In the end, this process of securitization produces results that differ significantly from the traditional model. The final feature of classic securitization is the application of exceptional, rule-breaking measures. According to Dunn Cavelty (2008), in both the concept of cybersecurity and the critically framed discourses applied therein, this process neither promotes martial law nor suspends democratic systems; such extreme measures may occur only rarely within oceanic domains. Instead, it leads to the formalization of security practices. Cybersecuritization institutionalizes novel regulatory schemas, territorializes surveillance apparatuses, and enacts a state of exception within a permanently militarized bureaucracy for cyber defense. The exceptional thus becomes the new bureaucratic normal (Cavelty & Egloff, 2019).

Bringing these concepts together, this research does not conceptualize cybersecuritization as a decisive and extraordinary halt of normal politics to combat a crisis in the *Indonesia's digital landscape*, but rather as a gradual, even banal, technocratic and deeply institutionalized risk management process. Theoretically, this narrative supports my analysis of a decade-long discourse in Indonesia's digital space by mapping how technical agencies articulate risks, how private and public actors negotiate representations of threats, and how these discourses ultimately provide rationales for new, permanent institutional infrastructures.

METHOD

This study used qualitative-descriptive methods, specifically employing a Critical Literature Review (Creswell & Creswell, 2018). The main subject of analysis was not the verbal or textual self-representations of state actors; therefore, post-structuralist techniques (e.g., CDA) were not required. In other words, this study approached the existing academic literature on Indonesia's cybersecuritization as its primary source of material. It qualitatively mapped the academic discourse using contextual keywords drawn from past research on securitization in the digital domain, including cyber threats in Indonesia. The literature was analyzed through thematic synthesis, observing how previous scholars had engaged securitization frameworks. This descriptive and critical assessment sought an academic exchange that recognized the empirical underpinnings of prior works while addressing theoretical blind spots and suggesting methodological refinements.

This study conducted a systematic search across Google Scholar, Scopus, and Elsevier databases using the following keywords: 'securitization,' 'cybersecuritization,' 'cyber threats Indonesia,' 'digital security Indonesia,' and 'Copenhagen School cybersecurity.' The search was limited to peer-reviewed publications between 2018 and 2025. Inclusion criteria required that articles (1) explicitly engaged with Securitization Theory or cybersecuritization frameworks, (2) focused on Indonesia's digital or cyber domain, and (3) were published in indexed academic journals. Exclusion criteria eliminated (1) non-academic grey literature, (2) purely technical cybersecurity papers without political or theoretical framing, and (3) works published before 2018.

From an initial pool of nine papers identified through keyword mapping, a two-stage filtering process was applied: first, filtering by engagement with securitization theory as an analytical lens; and second, verifying actual theoretical application in the analysis stage. This process resulted in five papers selected for in-depth critical analysis.

Table 1. The distribution of theme from selected literatures

Authors	***Keywords***	***Theoretical Framework***
(Lee, 2020)	Digitilization, Throttling, Shutdown, Hoax, Internet, Securitization Theory, Indonesia	Securitization theory
(Putri, 2023)	Harmful online content, securitization, freedom of speech	
(Azis & Azhari, 2025)	Illegal online gambling, Southeast Asia, Indonesia, Securitization, State Control	
(Wibowo et al., 2024)	Cybersecurity, Cyber Threats, Defense Strategy, Ministry of Defense, Securitization	

(Aji, 2025)	Cybersecurity Politics, Cyber Sovereignty, Governance, Institutions, BSSN, Policy Integration	State sovereignty theory & the theory of Cybersecurity Politics
(Arianto & Anggraini, 2025)	Indonesian National Cyber Forces, Geometripolitization, Securitization, Cyber Defence, Global Cyber Warfare	Geometripolitization and securitization theory
(Rai et al., 2022)	Balancer, Cybersecurity and Resilience, Free and Active, Mediator, Protectee	State Role theory
(Juned et al., 2024)	Bjorka, hacktivism, cybersecurity, cyberdemocracy, cyberactivism, Indonesia	Cyberactivism theory
(Aji, 2025)	Cyber Sovereignty, Cybersecurity, Revitalization, Political Will, Institutionalism, BSSN	Cyber Sovereignty theory

Source**:** Compiled and summarized from various literatures that emphasis their research on keywords, such as 'securitization,' 'digital domain,' and 'cyber threats in Indonesia'

From Table 1, initially this paper considered nine selected past literatures that shared the same nexus as the topic of this study, which were to be examined as the objects of our research. However, we were concerned with two levels of filters: (1) first, we aimed to establish an academic conversation later in the analysis stage of the paper only with past literature that actually engaged with the theoretical framework of securitization, either from the Copenhagen School or in its more progressive form of cybersecuritization; (2) second, we needed to further clarify whether the selected papers that declared the use of Securitization Theory as a keyword actually applied this perspective in their analysis stage. After a thorough review, we were left with only five academic papers as the main objects of analysis.

A renewed review of the literature identified a research position in the context of digital Indonesia that, to a certain degree, engaged with Securitization Theory. These papers did not use securitization as a strict analytical lens and sometimes treated it as if it were merely a passive backdrop, while at other times operating on assumptions that directly contradicted the constructivist core of the theory. The first tendency was to use securitization as nothing more than a vaguely defined conceptual framework rather than as a methodological tool. For example, Arianto (2025) attempted to contextualize the idea of cybersecurity within the Indonesian National Armed Forces (TNI) by offering localized approaches such as manunggalism and netika. However, the paper was weak in theoretical aspects even during the analytical stages, as it bypassed the broader securitization discourse. In this way, securitization became less of an active analytical lens and more of a frame, producing a narrative closer to an interpretation of future events than a theoretical inquiry, essentially, an informed prediction.

Second, empirical case studies within this cluster often fell into the trap of treating security as an objective reality, thereby completely missing the constructivist requirement of analyzing how threats were formulated. In parallel, Juned (2024) provided an informative account of the paradox of cyberdemocracy and the Bjorka hacktivism case. However, it was imperative to portray the theoretical foundation of hacktivism as its analytical framework in a separate section from the literature review. Despite using keywords such as "cyber-attack" and "threat," the authors did not explore the discursive construction of Bjorka's actions into a national cyber threat, leaving its definition open to interpretation, whether threats could be observed and addressed by objective (traditional) or subjective (expanded) means. Similarly, Aji (2025) focused their analysis on the National Cyber and Crypto Agency (BSSN) through the lens of cyber sovereignty, whereas Rai (2022) was more inclined toward assessing the role of the state (Indonesia) in shaping its national cybersecurity agenda.

RESULTS AND DISCUSSION

Results

Drawing the Mainstream: The Discourse of Cybersecuritization in Indonesia

Our assessment of cybersecurity discourse in Indonesia over the last five years begins with Lee's work, which emphasizes online hoaxes as the primary potential threat during Indonesia's presidential elections. In his theoretical framework, he attempts to synthesize

Balzacq's (2005) work, proposing that the components of Securitization Theory consist of six variables: (1) securitizing actor; (2) threat; (3) referent object; (4) audience; (5) context; and (6) state of exceptionality. In parallel, Azis (2025) emphasizes a tenet highlighted by Collins (2022), noting that securitization includes its first three sequences: (1) a non-politicized issue, in which securitizing actors have not yet acknowledged the weight of the threat; (2) a politicized issue, in which securitizing actors recognize the threat and direct it toward domestic political institutions; (3) a securitized issue, in which extraordinary responses are enacted to mitigate the threat and protect the identified referent object.

Whereas Putri's (2023) and Wibowo's (2024) papers adhere to the core principles of Securitization Theory, Aji's work (2025) seeks to further elaborate the process of a state's securitization by showing that the dynamics of domestic politics may influence how securitization unfolds. He emphasizes that political stability, drawing from Dunn (2020) work, functions as an important intervening variable that can shape the trajectory or outcomes of securitization efforts. Although his study provides limited contextual analysis of his specific case, it identifies six factors that may affect political stability before securitization occurs: (1) technology; (2) significant events (particularly cyber-related incidents); (3) international politics; (4) national politics; (5) academic debate; and (6) institutionalization. When all tenets are integrated into a single theoretical framework, the discourse of securitization effectively begins even before the formal process of securitization itself.

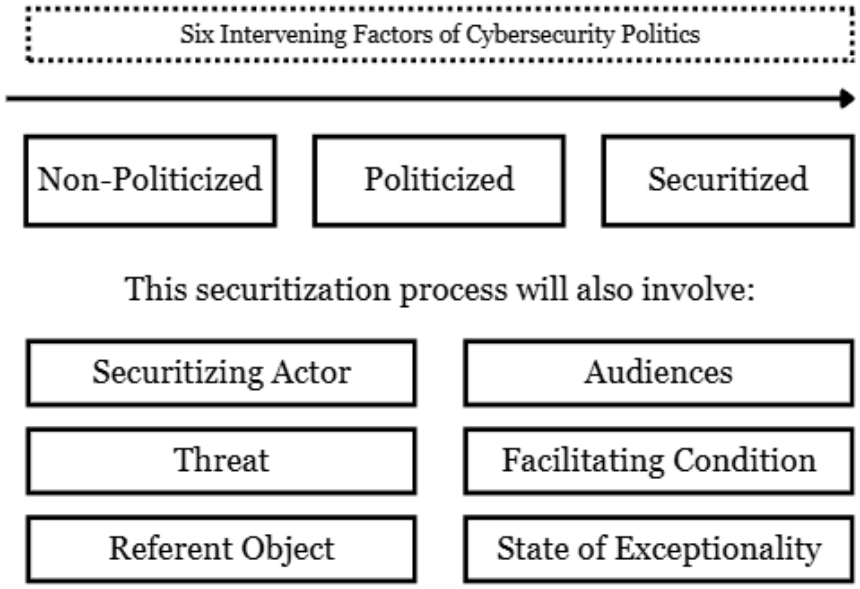

Figure 1. Summarizing Securitization's main tenets from the past academic discourse
Source**:** Compiled and summarized from various literatures

The figure 1 above showcases a synthesis of how the theoretical framework of securitization studies is applied in past literature (Aji, 2025; Azis & Azhari, 2025; Lee, 2020; Putri, 2023; Wibowo et al., 2024). Before securitization sets into motion, one may argue that attention should be given to the state's domestic politics. Since the state and its political agencies no longer possess maximum authority and knowledge regarding highly progressive problems in cyberspace, the process of an issue transforming from a non-politicized issue into a securitized issue is no longer centralized within the government. In Aji's work, he argues that a national institution, namely BSSN, can hold greater autonomy regarding the state's position against future digital crises if endowed with enhanced regulatory capacity compared to its previous form (2025). Notably, institutions such as the Ministry of Defense also bear responsibility for safeguarding Indonesia against future cyberthreats (Wibowo et al., 2024).

Although previous literature collectively agrees that the private sector lacks sufficient social capital to act as a securitizing actor for potential cyberattacks, Dunn Cavelty repeatedly stresses that technology-oriented and technocratic private sectors hold central authority should

a cyber threat become imminent. This contrasts with findings from 2018—though outside the main focus of this analysis—showing that Telkom Indonesia, Google, the Indonesian Internet Service Providers Association (APJII), and the Indonesian E-Commerce Association (idEA) Prayudi (2018), despite being identified as 'stakeholders' in the governance of cybersecurity in Indonesia, were never designated as responsible for securitizing Indonesia's cyber domain.

Shifting from the theoretical tenet to the components of theory, several findings illustrate how each is defined and referenced across different literature. First, a few studies strictly adopt the traditional view in defining 'securitizing actors,' referring to the general definition of "actors that declare." This definition has evolved to serve broader purposes: 'securitizing actors' must also guarantee the safeguarding of a country (Wibowo et al., 2024). Meanwhile, Wibowo (2024) does not strictly define or limit who qualifies as the 'ideal' securitizing actor during the securitization process. Lee (2020) suggests that this first component is not strictly limited to central governmental bodies; instead, 'securitizing agents' must possess social capital, specifically access to networks connecting to the public.

Conversely, Putri (2023) and Azis (2025) strictly limit securitizing agents to governmental bodies, political leaders, bureaucracies, lobbyists, and pressure groups, representing an almost entirely different paradigm. In a contrasting approach, Aji (2025) indicates, based on Prayudi (2018), that three domains of responsible stakeholders exist for cyber governance in Indonesia: Government, Private Sector, and Civil Society. While this expands the understanding of 'securitizing actors' beyond government and central authorities, Aji also emphasizes that a multivariate structure does not eliminate bureaucratic overlaps or the confusion of domain autonomy, which can hinder effective cyber crisis management. In summary, although most studies reference Buzan's definition of 'securitizing actors,' few adopt Dunn Cavelty's perspective on inclusivity and multiplicity, particularly within cyberspace. Dunn Cavelty emphasizes modern actors with fewer bureaucratic layers and greater technical expertise. Aji (2025) are the only scholars to recognize BSSN as a primary securitizing actor, reflecting technocratic tendencies, yet they do not explicitly incorporate Dunn Cavelty's framework.

The second finding this paper highlights concerns the second component of Securitization Theory: the 'speech act.' The Buzanian 'speech act' does not hold meaning independently; critics and subsequent developments, as emphasized by Vuori (2008), stress both (1) the sequence and (2) the types of strands in the declaration of speech.

Table 2. Strand types on identifying the purpose of Speech Act

No.	***Types of speech act***	***Forms of the speech act***
1.	Assertive speech act	Statements, explanations, and assertions
2.	Directive speech act	Orders, requests, and commands
3.	Commissive speech act	Vows, threats, and quarantines
4.	Expressive speech act	Apologies, thanks, and congratulations
5.	Declarative speech act	Declaring a war, pronouncing wedlock, and adjuring a meeting

Source: Vuori (2008)

Further highlighted by the table 2 above, the analysis stage of 'speech act' cannot finish right after the label is given to a certain speeches and declarations made by some political figure and their agencies, so therefore it will be classified as a 'speech act' processes; there are more inquiries that have to be made, for example, what purpose do these public speeches serve for the securitizing agents? what the literature has previously identified as a 'speech act'.

Table 3. Identification of the illocutionary types towards speech act

Authors	***Identified 'speech act'***	***Securitizing Actors***	***Explanation towards its purposes***
(Lee, 2020)	"Distributing hoax means to fire up hatred and open the case for the nation's Disintegration,"	Bambang Soesatyo, Indonesian House of Representative	*Available and explained, but the interpretation dose not referenceUnavailable and not explained* ***of*** *the purpose to any of the Language theory* (Balzacq,

		s	2005; Stritzel, 2007; Vuori, 2008)
	"It can disintegrate our nation, if hoax continues to spread, torn apart"	Joko Widodo, President of Indonesia	
	"the threat to the unity of Indonesia is not only posed by the military force but also other forces, such as radicalism, terrorism, intolerance, hoax, and cyberwar."	Tjahjo Kumolo, The Minister of Home Affairs	
	When people are threatened with hoaxes, to prevent them from going to the polling stations, that is considered a threat and an act of terror. For that reason, we will enforce Terrorism Law	Wiranto, Indonesian Coordinating Minister for Political, Law, and Security Affairs	
	"Hoax has recently been widespread and has become a threat to the societies. This power (hoax) is very tremendous, even more destructive than nuclear weapon,"	Air Chief Marshal Hadi Tjahjanto, The Indonesian Military Commander	
(Azis & Azhari, 2025)	"Gambling stakes the future, both personal, family, and our children's future. On the other hand, the government is seriously combating online gambling …"	Joko Widodo President of Indonesia	*Unavailable and does not explain of the purpose of each speech act done by the identified securitizing actors*
	"The government has announced its commitment to eradicating online gambling …"	The National Ministry of Communication and Information	
(Wibowo et al., 2024)	"Cyberattacks that can interfere with the sovereignty of the nation are currently wide open. Cyber army will consist of military, non-military and formed to ward off these attacks. We plan to form a cyber army. Every year we do cyber competitions and there are those who are specialized for defense or attack."	Purnomo Yusgiantoro, The Minister of Defense of Indonesia, in 2013	*There are two notes worthy to mention from this:* *1) The context of the study case and the illocutionary speech act done by the identified securitizing actors are outside of its time frame, rendering the speech act confusing to be utilized as a component of securitization theory* *2) There are no explicit explanations to what sort of purposes that the speech serves, especially with the securitization process.*
	"Cyber threats can be asymmetrical, where conflicts take place between one	Purnomo Yusgiantoro, The Minister of	

	nation whose cyber unit is developing and another nation whose is already very advanced. To anticipate this, we are now strengthening the defense force by developing our own cyber defense. The center is located at the Defense Ministry's headquarters in Pondok Labu, South Jakarta [...] "	Defense of Indonesia, in 2014	
	"We are also forming a cyber army. Every year we do this for cyber. Defense threats are not only traditional but also nontraditional ones. We prepare troops that have been sent to several countries—I can't say where—to conduct both attack and defense operations. [...] "		
(Putri, 2023)	-	-	*Unable to be identified*
(Aji et al., 2025)	*Not necessarily utilizing the Securitization Theory as its main theoretical lens, but emphasis its importance in his work* -		*Unable to be identified*

Source**:** Compiled and summarized from various literatures

Table 4. Comparative Evaluation of Selected Literatures Based on Securitization Theory Components

Author (Year)	Securitizing Actors Identified	Speech Act Typology Applied	Referent Object Defined	Dunn Cavelty Framework Utilized	Theoretical Rigor Assessment
(Lee, 2020)	Yes – state officials, military commanders	Partial – quotes identified but illocutionary analysis absent	Yes – national unity, election integrity	No	Moderate – applies Copenhagen School partially
(Putri, 2023)	Partial – government mentioned broadly	No – no speech act identified	Implicit – freedom of speech	No	Low – securitization used as backdrop
(Azis & Azhari 2025)	Yes – government, political leaders	Partial – state discourse cited without illocutionary analysis	Yes – national security, economic stability	No	Moderate – theoretical alignment but speech act gaps
(Wibowo et al.,	Yes – Ministry of	Partial – defense	Yes – state sovereignty,	No	Low – securitization

Author (Year)	Securitizing Actors Identified	Speech Act Typology Applied	Referent Object Defined	Dunn Cavelty Framework Utilized	Theoretical Rigor Assessment
2024)	Defense	statements quoted without temporal coherence	cyber defense		used loosely
(Aji et al., 2025)	Partial – BSSN as technocratic actor	No – securitization invoked but not applied	Yes – cyber sovereignty, BSSN mandate	Partial – cyber sovereignty cited alongside Dunn Cavelty	Moderate – multi-track framework, theory not fully operationalized

Source: Compiled by the author based on thematic analysis of reviewed literature

Some scholars successfully identify threat declarations but fail to anchor them in theoretical grammar. For instance, Lee (2020) catalogs numerous high-level statements regarding the threats of hoaxes and cyberwarfare from actors such as President Joko Widodo and the Indonesian Military Commander. However, the analysis merely presents these quotes at face value. The author provides explanations for the statements but entirely neglects to interpret them through the lens of foundational language theories, effectively stripping the speech act of its methodological rigor.

A second group of literature extracts quotes from state actors but fails to explain the operational purpose of the speech act within the securitization process. Azis (2025) highlight state discourse on online gambling, yet offer no explanation of what the speech act is intended to achieve (its illocutionary force). Similarly, Wibowo (2024) cite extensive historical remarks from the Minister of Defense regarding the formation of a cyber army. However, these statements are presented out of their original temporal context, and the authors fail to explicitly connect how these specific defense-oriented statements functioned as deliberate securitizing moves.

Most concerning are studies that claim securitization as a theoretical frame but abandon its methodology entirely. Works by Putri (2023) and Aji (2025) emphasize the importance of securitization in their respective studies, yet both do not identify any specific speech acts, actors, or referent objects. In these instances, securitization is reduced to a buzzword rather than an applied analytical lens, a Buzanian label of speech act.

CONCLUSION

With Indonesia's digital space already facing increasingly complex security challenges, there is an urgent need to move beyond largely anecdotal narratives and cultivate a more robust scholarly discourse. Although tracing state responses and the cyber tide is practically useful, a systemic view of the uneven power relations, political motivations, and institutional transformations behind these recurring phenomena requires an appropriate theoretical framework applied rigorously. Motivated by this need, the main aim of this paper was to reassess the existing literature on Indonesia cybersecuritization to delineate how such academic phenomena are evolving. Drawing on a qualitative-descriptive methodology that treats the literature as the primary object of analysis, this research revealed that although scholarly publications have urgently called attention to existential concerns over digital threats and policy transformations, their theoretical implementation is ultimately at odds with the nature of cyberspace.

The original flaw lies in theoretical simplification coupled with reliance on outdated, 'old-world' models. Securitization in the literature is often treated as a passive backdrop or jargon rather than as an active analytical tool. This paper argues that the existing literature, which constitutes the objects of analysis, consistently imposes Buzanian state-centered models of digital "existential threats" onto the cyber domain while overlooking the increasingly technocratic and

risk-management-driven modus operandi in contemporary cyber governance. Perhaps most crucially, the use of the "speech act" concept has been entirely stripped of critical merit. The literature reviewed frequently conflates political public rhetoric with concerted securitizing moves, often parsing locutionary performatives at face value while insufficiently deconstructing their illocutionary purpose, context, and sequencing.

A methodological recalibration to address these theoretical blind spots. Future scholarly work must cease treating cyber threats as objective, pre-constructed realities and return to the constructivist core of Securitization Theory. The linguistic precision of speech act deconstruction, emphasized by Vuori, must be integrated with Dunn Cavelty's model of cybersecuritization, a nascent branch of contemporary securitization studies. This two-pronged lens enables the broader academic community to recognize non-traditional, technocratic securitizing actors and to develop a more nuanced understanding of how language on digital vulnerabilities is mobilized to justify the bureaucratic institutionalization of cybersecurity in Indonesia.

Finally, while this systematic review highlights serious methodological concerns in prior studies, it must also acknowledge its own analytical limitations. This paper serves primarily as a critique with a focused examination of specific data, limited to three core components of the theory: securitizing actors and speech acts. Consequently, a comprehensive mapping of Indonesia's cybersecuritization discourse remains a work in progress. Future research is strongly encouraged to build upon this groundwork and systematically examine the remaining aspects of the cybersecuritization framework. By operationalizing this framework (through systematic diagnosis of threat construction, identification of referent objects, critical audience reception, and evidence of state exceptionality/institutionalization) scholars can ensure that Indonesia's digital security discourse evolves into a fully developed, rigorous, and dynamic scientific debate.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Universitas Pembangunan Nasional Veteran Jakarta (UPN Veteran Jakarta) for providing academic support and an intellectual environment that facilitated the completion of this study. The authors also appreciate the scholars and researchers whose works on securitization theory, cybersecuritization, and cybersecurity governance contributed significantly to the development of the analytical framework employed in this research. Special thanks are extended to colleagues and peer reviewers for their constructive feedback and valuable suggestions, which helped improve the quality and rigor of this manuscript. Any remaining errors or interpretations are solely the responsibility of the authors.

AUTHOR CONTRIBUTION STATEMENT

Kamil Ghiffary A: Conceptualization, literature review design, theoretical framework development, data collection, thematic analysis, interpretation of findings, writing – original draft preparation, and manuscript revision. Hartanto: Research supervision, methodology validation, theoretical review, critical analysis, writing – review and editing, and manuscript refinement. Ivandra Solihin: Literature screening, data organization, validation of findings, reference management, manuscript editing, and final review.

REFERENCES

Aji, M. P. (2025). Cybersecurity Politics in Building Cyber Sovereignty in Indonesia Through Strengthening the Role of the National Cyber and Crypto Agency. *Society*, *13*(2), 1056–1071. https://doi.org/10.33019/society.v13i2.960

Aji, M. P., Somantri, G. R., & Rofii, M. S. (2025). Building Cyber Sovereignty in Indonesia Through Revitalization of the National Cyber and Crypto Agency of the Republic of Indonesia. *Journal of Cultural Analysis and Social Change*, 1275–1283. https://doi.org/10.64753/jcasc.v10i2.1771

Arianto, A. R., & Anggraini, G. (2025). Pembentukan TNI Angkatan Siber dalam Perspektif Teori Geometripolitisasi (Mazhab Indonesia) dan Sekuritisasi (Mazhab Kopenhagen) terhadap Ruang Siber di Indonesia untuk Menghadapi Perang Siber Global. *Ilmu Dan Budaya*, *46*(2), 109–125.

Azis, A. A., & Azhari, M. I. (2025). Illegal online gambling in Indonesia: Assessing state securitization and its effectiveness. *Jurnal Hubungan Internasional*, *14*(1), 1–14.

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context. *European Journal of International Relations*, *11*(2), 171–201.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cavelty, M. D. (2012). The militarisation of cyberspace: Why less may be better. *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–13.

Cavelty, M. D., & Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, *15*(1), 37–57.

Collins, A. (2022). *Contemporary security studies*. Oxford University Press.

Creswell, J. W., & Creswell, J. D. (2018). Research Design Qualitative, Quantitative, and Mixed Methods Approaches. In *Sage Publications, Inc.* (5th ed., Issue 2).

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122.

Dunn Cavelty, M., & Wenger, A. (2020). Cybersecurity meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Fauzi, E., Citra, H., Marwenny, E., & Alfitrianti, N. (2024). Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty. *Jurnal Ilmiah Ekotrans & Erudisi*, *4*(1), 149–157.

Febriawan, D., & Marisa, H. (2024). Understanding Indonesia's cybersecurity policies: Opportunities and challenges in the digitalization transformation era. *JOELS: Journal of Election and Leadership*, *5*(1), 13–21.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cybersecurity, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Juned, M., Martin, A., & Pratama, N. (2024). Bjorka's Hacktivism in Indonesia: The Intercourse Paradox of Cyberdemocracy, Cyberactivism, and Cybersecurity. *Academic Journal of Interdisciplinary Studies*, *13*(5), 369–380.

Kurniawan, Y. (2018). *The politics of securitization in democratic Indonesia*. Springer. https://doi.org/10.1007/978-3-319-62482-2

Lee, A. (2020). Online hoaxes, existential threat, and internet shutdown: a case study of securitization dynamics in Indonesia. *Journal of Indonesian Social Sciences and Humanities*, *10*(1), 17–34.

Prayudi, P., Budiman, A., Ardipandanto, A., & Fitri, A. (2018). *Keamanan siber dan pembangunan demokrasi di Indonesia*. Pusat Penelitian Badan Keahlian DPR RI.

Putri, T. E. (2023). Government Securitizing Effort of Online Harmful Content in Indonesia. *Komunikasi: Jurnal Komunikasi*, *14*(2), 224–232. https://doi.org/10.31294/jkom.v14i2.12018

Qiao-Franco, G. (2024). An emergent community of cyber sovereignty: the reproduction of boundaries? *Global Studies Quarterly*, *4*(1), ksad077. https://doi.org/10.1093/isagsq/ksad077

Rai, I. N. A. S., Heryadi, D., & Kamaluddin, A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(1), 43–66. https://doi.org/10.22212/jp.v13i1.2641

Reindl, A. P. (1998). Choosing Law in Cyberspace: Copyright Conflicts on Global Networks. *Michigan Journal of International Law*, *19*(3), 799–871.

Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations*, *13*(3), 357–383.

Taylor, R. D. (2022). Preserving human rights across the digital domain. *Available at SSRN 4178327*.

Vuori, J. A. (2008). Illocutionary logic and strands of securitization: Applying the theory of securitization to the study of non-democratic political orders. *European Journal of International Relations*, *14*(1), 65–99.

Wibowo, S. E., Hartono, A., Kiswanto, H., Louerens, J. T. A., & Primawanti, H. (2024). Securitization of Cyber Threats to the Indonesian Government: A Study of Cyber Defense Strategy. *Global Political Studies Journal*, *8*(2), 97–108. https://doi.org/10.34010/gpsjournal.v8i2