Received: 1 November 2025 | Revised: 11 January 2026 | Accepted: 9 April 2026

Papua Journal of Diplomacy and International Relations
Volume 6, Issue 1, May 2026 (43-67)
DOI : 10.31957/pjdir.v6i1.5041
ISSN 2797-0957 (Online)

Cybersecurity Vulnerabilities at the Indonesia–Papua New Guinea Border: Securitization Asymmetry, Institutional Gaps, and Diplomatic Escalation

Dewi Anjani Kartika Putri* | **Ali Maksum**

INSTITUTION/ AFFILIATION

Department of International Relations, Faculty of Social and Political Sciences, Universitas Muhammadiyah Yogyakarta, Yogyakarta, Indonesia

CORRESPONDENCE

*Dewi Anjani Kartika Putri, Universitas Muhammadiyah Yogyakarta, Jl. Ring Road Selatan, Geblagan, Tamantirto, Kec. Kasihan, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55184, Indonesia
Email: dewi.anjani.psc24@mail.umy.ac.id

ABSTRACT

This study aims to examine how cybersecurity vulnerabilities at the bilateral border between Indonesia and Papua New Guinea (PNG) create risks of diplomatic crises through institutional gaps and asymmetric threat perceptions. By adopting a qualitative research approach, and drawing on securitization theory and constructivism in IR, this article reveals four key findings. First, Indonesia and PNG lack formal bilateral agreements on cyber incident response and attribution procedures. Second, asymmetric securitization exists whereby Indonesia over-securitizes cyber threats while PNG under-securitizes them, creating misaligned threat perceptions. Third, the absence of shared norms prevents a coordinated bilateral response. Fourth, historical trust deficits facilitate rapid escalation from technical incidents to diplomatic crises. Theoretically, these findings demonstrate how securitization asymmetry operates at the bilateral level, and practically, they identify mechanisms for preventing cyber incidents from disrupting diplomatic stability in the Indo-Pacific.

KEYWORDS

Border; Cybersecurity Vulnerabilities; Indonesia; Papua New Guinea; Securitization Asymmetry

INTRODUCTION

The way countries regulate the cross-border flow of people, goods, and information has changed significantly due to the digitization of border management systems. Contemporary border posts are increasingly dependent on interconnected digital infrastructure, such as biometric identification systems, customs databases, immigration records, and security communication networks. While digital transformation improves administrative efficiency and security, it also creates new vulnerabilities. Cyberattacks on border infrastructure can paralyze operations and threaten diplomatic stability between neighboring countries. This is especially true in cases where bilateral cooperation mechanisms have not been developed to deal with cyber incidents (Thumfart, 2022) .

This challenge is particularly urgent along the Indonesia-Papua New Guinea (PNG) border, where significant cybersecurity asymmetries, recent geopolitical realignments, and institutional cooperation gaps converge to create unprecedented diplomatic risks. Indonesia is currently facing one of the most severe cybersecurity crises in Southeast Asia, experiencing an average of 3,300 cyberattacks per week in 2024-2025 and recording 3.8 billion traffic anomalies over the past five years (Yuniar, 2025). The ransomware attack on June 20, 2024, against Indonesia's Temporary National Data Center (PDNS), which disrupted 282 government services, including immigration and airport systems, for several days, demonstrates the catastrophic potential of cyber vulnerabilities in critical infrastructure. This "Brain Cipher" ransomware variant of LockBit 3.0 caused the loss of backup data and a ransom demand of $8 million, which was rejected by the Indonesian government (Nugroho, 2024) .

Meanwhile, Papua New Guinea recently launched its National Cyber Security Strategy (NCSS) 2024-2030 in March 2025 (Dept of Information & Communication Technology, 2023), with implementation still in its early stages, creating a substantial disparity in cyber readiness between the two neighboring countries. The signing of the Pukpuk Treaty in October 2025, the first defense agreement between Australia and Papua New Guinea in seven decades, further increases the strategic significance of the Indonesia-PNG border in the context of great power competition in the Indo-Pacific. This geopolitical shift transforms what were previously routine administrative border crossings at the Skouw (Jayapura) and Sota (Merauke) border posts—used here as a representative example—into potential flashpoints where cyber incidents could trigger diplomatic crises and security escalations (see Figure 1).

The Skouw Border Post, which was inaugurated on May 9, 2017, has evolved into a strategic trade terminal with modern digital infrastructure, including an integrated Customs, Immigration, Quarantine, and Security (CIQS) system, facial recognition technology, and cargo scanning facilities. At the regional level, Papua's total exports reached US$12.85 million in May 2025, a 135.39% increase from the previous month, signaling rising economic activity surrounding cross-border trade (Central Bureau of Statistics of Papua Province, 2025).

In contrast, the Sota Border Crossing Point (PLBN), inaugurated on October 3, 2021, represents a different configuration of border development, operating within a more asymmetrical institutional environment and supported by integrated CIQS facilities (Metherall et al., 2022; Pugu & Pusung, 2025). Together, these two border posts illustrate how varying levels of infrastructure development and institutional capacity shape the cybersecurity landscape along the Indonesia–Papua New Guinea border.

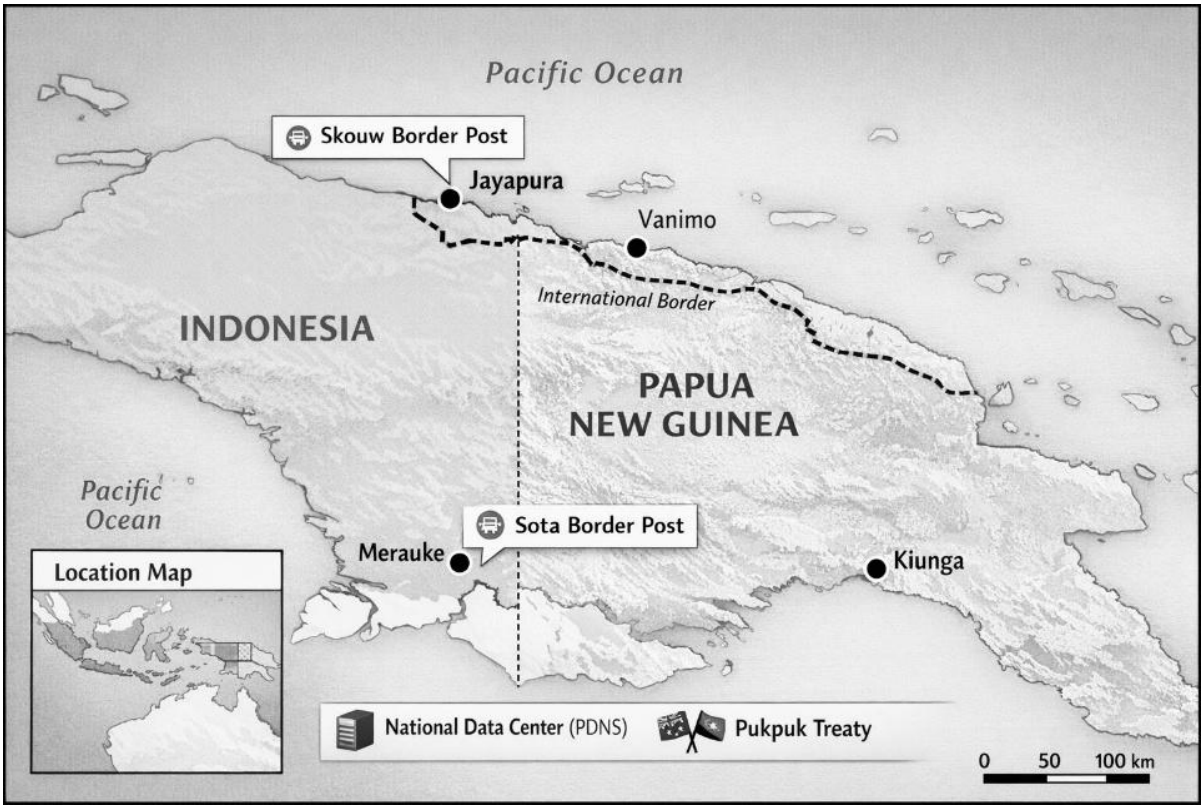

Figure 1. Geographic location of Skouw (Jayapura) and Sota (Merauke) border posts along the Indonesia–Papua New Guinea border.

Source: Author's illustration based on geographic data from OpenStreetMap and Natural Earth, with location references from Google Maps (2026)

Despite growing recognition of the importance of cybersecurity in international relations and the ongoing digitization of border management, the specific intersection between cyber vulnerability and border diplomacy remains largely unexplored. Existing cybersecurity research largely focuses on national-level threats or global cybersecurity governance frameworks, rarely examining how cyber incidents on shared border infrastructure affect bilateral diplomatic relations (Buchanan, 2017; Buchkovska, 2025; Robinson, 2024). Border studies literature also neglects the cyber dimension, while international relations theory has not adequately conceptualized the mechanisms by which cyber vulnerability translates into

diplomatic instability (Gunawan et al., 2024; Souisa & Renaldi, 2025; Sumadinata et al., 2022).

This research gap has significant practical implications. Without understanding how cyber incidents on border infrastructure can escalate into diplomatic crises, policymakers lack the analytical framework necessary to develop appropriate bilateral cooperation mechanisms, incident response protocols, and confidence-building measures. The absence of such a framework becomes particularly dangerous when the technical challenges of attribution—inherent in cyber incidents—combine with pre-existing trust deficits and geopolitical tensions, creating conditions for blame games and diplomatic damage.

The Indonesia-PNG border case represents an ideal context for addressing this gap, given the documented cyber asymmetry between the two countries, the absence of bilateral cyber cooperation protocols, recent geopolitical shifts following the Pukpuk Treaty, and strategic interests in Indo-Pacific power competition. Specifically, critical border infrastructure at the Skouw and Sota border posts operates with documented vulnerabilities, while bilateral mechanisms for managing cyber incidents are still absent, creating a scenario in which cyber attacks could quickly escalate beyond technical disruptions to threaten diplomatic stability.

Although there is a Memorandum of Understanding (MoU) between Indonesia and PNG on cross-border transportation cooperation signed in July 2024 (Korwa & Rumabar, 2024), there is no specific bilateral agreement governing cybersecurity cooperation or cyber incident response protocols at the border. At a broader level, although Indonesia and Australia signed an MoU on Enhancing Cybersecurity and Critical Technology Cooperation on August 28, 2025, a similar agreement between Indonesia and PNG does not yet exist, leaving a critical institutional gap in the regional cybersecurity architecture (Marles et al., 2025).

Therefore, this study poses the following main research questions: How does the interaction between securitization asymmetry, institutional gaps, and cybersecurity vulnerabilities at the Indonesia-PNG border create risks of diplomatic escalation, and what bilateral institutional mechanisms and confidence-building measures can effectively mitigate these risks?

This study makes three interconnected contributions to scholarship on cyber-diplomatic crises at bilateral borders. First, theoretically, it is the first to systematically integrate Securitization theory and Constructivism in International Relations (IR) to analyze the cyber-border-diplomacy nexus, revealing how asymmetric threat perception interacts with institutional gaps to create escalation risks. While securitization theory and constructivism have been applied separately to cybersecurity contexts in prior scholarship, their combination to explain bilateral institutional gap formation in the cyber-border context remains novel and underexplored in IR literature. Second, empirically, this study identifies specific institutional vulnerabilities and securitization dynamics at the Indonesia-PNG

border that have received limited scholarly attention despite their strategic significance in the broader context of Indo-Pacific geopolitical competition and great power dynamics. Third, practically, this study provides policymakers with concrete, theoretically-grounded recommendations for establishing bilateral cyber cooperation frameworks, building shared understanding of cyber threats through sustained official dialogue, and implementing confidence-building measures to prevent technical cyber incidents from disrupting diplomatic stability and regional security in the Indo-Pacific.

This article proceeds as follows. Following this introduction, we present our theoretical framework, integrating securitization theory from the Copenhagen School and Constructivism to analyze the mechanisms through which cyber vulnerabilities interact with institutional gaps and threat perception asymmetries. We then describe our qualitative research methodology, including our document analysis approach, specific data sources from Indonesia's BSSN and Papua New Guinea's DICT, and our analytical frameworks. The results and discussion section is organized around three key dimensions that emerged from our analysis: first, institutional and infrastructure vulnerabilities on the Indonesia-PNG border and the documented cyber asymmetries between the two countries; second, asymmetric securitization dynamics whereby Indonesia and Papua New Guinea construct cyber threats differently based on their institutional capacities and threat perception frameworks; and third, the role of identity construction, absent shared norms, and historical trust deficits rooted in past tensions over migration, maritime boundaries, and resource management in creating conditions for rapid escalation from technical incidents to diplomatic crises. Finally, our conclusion synthesizes these findings, addresses limitations of the study, and proposes specific institutional and diplomatic mechanisms for bilateral cyber cooperation and confidence-building that can enhance regional security in the Indo-Pacific context.

THEORETICAL FRAMEWORK

Given our research question examines how securitization asymmetry and institutional gaps at the Indonesia-PNG border create risks of diplomatic escalation, we structure our literature review and theoretical framework around three dimensions. First, we examine research on cybersecurity vulnerabilities at critical border infrastructure and how digital dependencies create new risks. Second, we review scholarship on institutional capacity asymmetries in cybersecurity, showing how countries with different capacities have divergent threat perceptions. Third, we analyze literature on how asymmetric threat perception and absent shared norms impede bilateral cooperation and can escalate to diplomatic crises. This three-part structure ensures our theoretical frameworks are directly responsive to understanding our specific case.

Research on border security and cybersecurity remains a relatively separate area in academic literature. The most fundamental gap is the absence of academic publications that

comprehensively analyze the intersection between cybersecurity vulnerabilities, border security, and bilateral diplomatic stability in the specific context of Indonesia-Papua New Guinea. A Scopus search using the keyword combination "cyber" AND "Indonesia" AND "Papua" yielded only four publications over a seven-year period, and significantly, none of these four publications analyzed cybersecurity threats to critical border infrastructure or the diplomatic implications of cyber incidents. The four publications focus on different topics: cyberactivism in the context of West Papua activism (Asemki et al., 2023), cyber law aspects and internet restrictions from a human rights perspective (Putra, 2022), journalistic collaboration in reporting on the Papua conflict (Abrar, 2021), and the potential of cyber technology in regional economic development (Berawi et al., 2017). The absence of literature on the cyber-border-diplomacy nexus indicates that although the three dimensions of cyber security, border security, and bilateral diplomacy each have established literature, their integration in the context of Indonesia-PNG remains largely unexplored in international academia.

At a broader level, research on border security shows that digital technology is becoming increasingly important in supporting modern border operations (Gunawan et al., 2024). Studies on cybersecurity from an institutional capacity perspective show that countries with limited institutional capabilities face different challenges in implementing cybersecurity frameworks (Buchkovska, 2025). The gap between developed and developing countries in terms of cybersecurity capacity creates significant asymmetries in threat perception and response mechanisms. Critical to our analysis is understanding how cybersecurity capacity asymmetries translate into asymmetric securitization. When one country (Indonesia) has greater institutional capacity and perceived cyber threats, while another (PNG) has limited capacity and underdeveloped threat frameworks, the result is not simply a difference in cybersecurity posture but a fundamental asymmetry in how each country constructs the meaning and urgency of cyber threats. This asymmetry has direct implications for bilateral cooperation, frameworks established by the over-securitizing state are perceived as unnecessary or threatening by the under-securitizing state, creating conditions for misunderstanding and escalation.

The literature on cyber diplomacy shows that the absence of universally accepted frameworks for cyberspace governance poses a fundamental challenge (Buchkovska, 2025; Robinson, 2024). Cyber diplomacy, defined as the use of diplomatic tools to manage and resolve issues in cyberspace, is still in its early stages of development, particularly in the context of bilateral relationships between countries with asymmetric capacities. Research on international relations and threat perception shows that when countries with different capacities do not have shared frameworks for understanding threats, the probability of misinterpretation and escalation increases significantly (The U.S. Intelligence Community, 2025). By integrating insights from this literature, this study fills a significant gap by

specifically analyzing the nexus between cybersecurity vulnerabilities, border security, and diplomatic stability in the context of bilateral relations between Indonesia and PNG.

This study uses two main theoretical frameworks to analyze the nexus between cybersecurity, border security, and bilateral diplomacy. First, Securitization Theory from the Copenhagen School explains that issues can be elevated from the normal political domain to security issues through speech acts and framing by actors with authority (Buzan et al., 1998). Critically for our analysis, securitization is not an objective process reflecting actual threats but a socio-political construction in which meanings and urgency of threats are created through discourse and political framing.

Securitization theory specifically illuminates our case of the Indonesia-PNG border. Indonesia, with its greater institutional capacity, including a structured National Cyber and Cryptography Agency (BSSN), military involvement in cybersecurity, and an established National Cyber Security Strategy, tends to over-securitize cyber threats, constructing them as existential security issues requiring extraordinary measures beyond normal political procedures. This over-securitization is visible in Indonesia's intensive response to the June 2024 PDNS ransomware attack, which was framed as a national security crisis requiring military-technical coordination. Conversely, Papua New Guinea, with limited institutional capacity and a National Cyber Security Strategy only recently launched in 2025 still in early implementation stages, tends to under-securitize cyber threats. PNG does not yet construct cyber threats with the same urgency, viewing them more as technical issues for gradual capacity building rather than as existential security threats requiring immediate extraordinary measures.

This asymmetry in securitization processes directly explains the institutional gap we observe at the bilateral level. When one country securitizes an issue while the other does not, bilateral cooperation frameworks fail to materialize because the countries operate from fundamentally different threat constructions and urgency perceptions. Indonesia's over-securitization creates institutional pressure for formal bilateral frameworks, stringent security measures, and military-technical coordination. PNG's under-securitization means PNG perceives such frameworks as unnecessary or potentially intrusive. The result is institutional gap formation, the absence of bilateral agreements on cyber incident response, attribution procedures, and diplomatic communication channels. This gap emerges not merely from capacity differences but from asymmetric securitization creating misaligned expectations about the necessity and appropriateness of bilateral institutions. Bilateral frameworks established by the over-securitizing state (Indonesia) are perceived by the under-securitizing state (PNG) as excessive or unilaterally imposed rather than mutually beneficial, preventing agreement formation.

Second, Constructivism in International Relations emphasizes the role of identity, social norms, and intersubjective understanding in shaping state behavior (Wendt, 1995). For our analysis, constructivism reveals how institutional gaps in bilateral cyber cooperation

emerge not only from capacity asymmetries but from underlying asymmetries in threat identity construction and from the absence of shared norms.

Specifically, constructivism illuminates a critical mechanism. When two states have not developed a shared understanding of what cyber threats mean and how they should respond, they lack the intersubjective foundation necessary for building bilateral institutions. The absence of shared norms about cyber incident attribution procedures, incident response protocols, diplomatic communication channels, and escalation management means that technical cyber incidents cannot be managed through established procedures. Instead, each incident becomes an isolated event interpreted through each country's own frameworks, creating opportunities for misattribution, blame games, and security dilemma dynamics. For example, if Indonesia detects a cyber intrusion and proposes enhanced border monitoring to identify the threat source, PNG might interpret this defensive measure as a threat to PNG's sovereignty rather than as protective cooperation. Without shared norms defining what constitutes appropriate responses to cyber incidents, defensive measures by one state are misinterpreted as offensive preparations by the other.

Constructivism explains that such norms do not emerge automatically but must be deliberately constructed through dialogue, interaction, repeated coordination, identity alignment, and advocacy by norm entrepreneurs. At the Indonesia-PNG border, however, the historical trust deficits rooted in migration tensions, maritime boundary disputes, and resource management issues have prevented the identity convergence necessary for bilateral norm-building. Indonesia constructs itself as a more advanced cybersecurity actor, while PNG constructs itself as a developing country requiring capacity assistance. This identity asymmetry creates reluctance on both sides: Indonesia may be reluctant to treat PNG as an equal partner in bilateral frameworks, while PNG may be reluctant to participate in frameworks perceived as one-way assistance rather than cooperation. Without shared identities regarding appropriate bilateral roles, and without the historical trust foundation that enables norm-building, the two countries cannot develop the shared norms necessary for effective cyber incident response.

The integration of securitization theory and constructivism enables comprehensive analysis of how technical vulnerabilities interact with political and social dimensions to create diplomatic escalation risks at the bilateral level. Securitization theory explains the macro-level political processes whereby asymmetric threat perception emerges and prevents bilateral cooperation. Constructivism explains the micro-level social processes whereby absent shared norms and identity misalignment prevent norm-building and trust development. Together, these frameworks illuminate the complete escalation mechanism.

Specifically, the two theories show that cybersecurity vulnerabilities alone do not cause diplomatic crises. Rather, technical vulnerabilities combined with asymmetric securitization and absent shared norms create conditions where technical incidents rapidly

escalate to diplomatic confrontations. Consider a hypothetical scenario: if a cyber intrusion occurs at the Skouw or Sota border post, Indonesia, operating from an over-securitized threat construction—may immediately interpret this as a strategic cyber threat requiring rapid response and potential military-technical coordination. PNG, operating from an under-securitized threat construction and lacking shared incident response norms with Indonesia, may see Indonesia's response as an overreaction or even as preparation for military action. Without shared norms defining appropriate response procedures, and without identity alignment creating mutual understanding, the technical incident rapidly escalates into a diplomatic dispute as each country misinterprets the other's actions through incompatible threat lenses.

This integrated theoretical framework also identifies intervention points for policy. Addressing cybersecurity risks at the bilateral border requires not only technical measures (improving cyber defenses at border infrastructure) but diplomatic and social measures: dialogue to build shared understanding of threat perceptions, norm-building to establish bilateral protocols for cyber incident response and attribution, and confidence-building measures to signal non-hostile intent and reduce the security dilemma dynamics. The framework shows that sustainable resolution requires working simultaneously at the technical level (reducing vulnerabilities), the political level (aligning securitization perceptions), and the social level (building shared norms and identity alignment).

METHODS

This study uses a qualitative approach with a literature review (document analysis) method to analyze the intersection between cybersecurity vulnerability, border security, and diplomatic stability on the Indonesia-Papua New Guinea border. The qualitative approach was chosen because of its suitability for the research objectives, which sought to understand complex phenomena through in-depth interpretation of textual and contextual data, as recommended by Braun and Clarke (2021) in research requiring a nuanced understanding of social and political constructs. The document analysis method, as a systematic qualitative research technique, allows researchers to identify, analyze, and interpret relevant documents in order to comprehensively answer research questions (Bowen, 2017; Nurisnaeny et al., 2025).

The primary data sources for this study include cybersecurity policy documents from Indonesia's National Cyber and Cryptography Agency (BSSN) and Papua New Guinea's Department of Information and Communication Technology (DICT), documented cybersecurity incident reports, and bilateral agreements between Indonesia and PNG regarding border cooperation. Secondary data was obtained from Scopus-indexed journal articles, international organization reports, think tank publications, and official government documents related to cybersecurity, border security, and Indonesia-PNG diplomatic relations in the period 2018-2025. This time frame was chosen based on significant

developments in the regional cybersecurity landscape and fundamental geopolitical changes in the Indo-Pacific, particularly in the wake of the COVID-19 pandemic, which accelerated the digitization of border infrastructure, and the signing of the Pukpuk Treaty in October 2025, which changed the dynamics of regional security (Praditya et al., 2023).

Data collection was conducted systematically by searching the Scopus academic database, Google Scholar, and institutional repositories using a combination of the keywords "cyber", "Indonesia", and "Papua". Policy documents were accessed through the official websites of BSSN (bssn.go.id), DICT PNG (ict.gov.pg), and the Ministries of Foreign Affairs of both countries. Document inclusion criteria included relevance to the research topic, source credibility, and adequate data availability for analysis. The documents used include the Indonesian national cybersecurity strategy (National Cybersecurity Strategy 2023-2028) and PNG (National Cyber Security Strategy 2024-2030), cyber incident reports from BSSN and related agencies, and the bilateral Memorandum of Understanding between Indonesia and PNG. In addition, this study analyzes specific case studies such as the PDNS ransomware attack in June 2024 and the digital infrastructure at the Skouw and Sota border crossing points (see Figure 1) as representations of cyber vulnerabilities in border infrastructure (Chaudhuri et al., 2025; Kaifa et al., 2025).

RESULTS AND DISCUSSION

Institutional and Infrastructure Vulnerabilities

The Skouw (Jayapura) and Sota (Merauke) border posts are modern facilities that depend on interconnected digital systems to manage the cross-border movement of people and goods. Key components include biometric identification systems (e-gates, fingerprint and facial scanners), an immigration database connected to Indonesia's national system, an electronic customs platform (Indonesia National Single Window/INSW), integrated surveillance systems (CCTV), and internal communication networks (LAN/WAN and radio/VoIP for inter-agency coordination). Because these systems connect vertically to national-level infrastructure, both PLBNs function as critical nodes in Indonesia's wider border security architecture (Souisa & Renaldi, 2025).

This vertical dependence, however, also creates systemic exposure: disruptions at the national level can cascade down to border operations. The June 2024 ransomware attack on Indonesia's Temporary National Data Center (PDNS) disrupted 282 government services (Nugroho, 2024), including immigration and airport systems, for several days. While publicly available reporting does not specify direct impacts on Skouw or Sota, the incident demonstrates how centralized digital dependencies can translate into operational fragility at peripheral sites. Importantly, the PDNS case also surfaced weaknesses related to backups and incident response that may plausibly extend to other government-connected infrastructures, including border facilities (Johnson & Ziogas, 2024).

A further challenge is the limited availability of publicly accessible technical detail on cybersecurity protections at Skouw and Sota. In the absence of official technical disclosures, assessment must remain cautious and inferential. Nevertheless, standard cybersecurity practices for modern border facilities typically include layered controls such as firewalls, virtual private networks (VPNs), network segmentation, routine data backups, physical access control, encrypted communications, and defined incident response procedures (Wickham, 2025). At the strategic level, Indonesia has introduced a National Cyber Security Plan (2023–2028) through BSSN, while Papua New Guinea has launched a National Cyber Security Strategy (2024–2030). Yet, in both contexts, implementation maturity at the border-operational level remains difficult to verify from open sources, indicating persistent uncertainty regarding readiness for cyber incidents at PLBN sites (Rainforest Rescue, 2025).

The most consequential vulnerability is institutional rather than purely technical, the absence of a dedicated bilateral cybersecurity cooperation framework between Indonesia and PNG. Although the two countries maintain memoranda of understanding on border cooperation (including a transport MoU dated July 2024), there is no formal protocol designed to manage cyber incidents affecting shared or interdependent border infrastructure (Hutagalung, 2024). This gap is particularly evident across four dimensions. First, there is no jointly agreed cyber incident response protocol specifying communication pathways, escalation procedures, and role division during an attack (The European Union Agency for Cybersecurity, 2024). Second, no structured information-sharing mechanism exists for exchanging cyber threat intelligence relevant to border security (Alaeifar et al., 2024), despite the importance of shared early warning for preventive action (Busetti & Scanni, 2025). Third, there are no agreed attribution procedures to reduce the risk of misattribution and blame games, which can quickly damage bilateral relations (Rupp & Paulus, 2023). Fourth, the absence of dedicated diplomatic communication channels for crisis situations increases the likelihood of miscommunication and unnecessary escalation (CCB, 2021).

This institutional asymmetry becomes clearer when contrasted with Indonesia's cooperation patterns elsewhere. Indonesia signed a cybersecurity cooperation MoU with Australia on August 28, 2025. The presence of this Indonesia–Australia arrangement, alongside the absence of a comparable Indonesia–PNG framework, suggests that cybersecurity cooperation with PNG has not yet been consolidated as a bilateral priority, despite the shared land border and increasing digitization of border operations (Costa, 2024).

Skouw-Wutung Border Post

The Skouw Border Post in Jayapura serves as an integrated border post that combines immigration, customs, and quarantine services within Indonesia's national border management system (Pugu et al., 2019). Physically, this site is designed as a modern cross-

border complex equipped with integrated Customs, Immigration, Quarantine, and Security (CIQS) facilities, checkpoints, and commercial areas that support cross-border mobility and daily trade activities. This post serves as a direct interface with Papua New Guinea and has evolved into a key hub for cross-border mobility and local economic exchange (Metherall et al., 2022). Beyond its physical role, the facility operates within a broader framework of coordinated governance and increasingly relies on national administrative and digital infrastructure for security, customs, and regulatory processes (Harefa & Supriyadi, 2025; Sumadinata et al., 2022).

One of Skouw's distinctive features is its institutional partnership with Wutung on the Papua New Guinea side, which enables direct operational coordination between border authorities, an arrangement not found at border posts that lack official partners (Harefa & Supriyadi, 2025; Wallis et al., 2025). This institutional pairing has analytical significance because it can reduce uncertainty during disruptions and enable faster cross-border communication compared to asymmetric border arrangements. In practice, communication during incidents is primarily conducted through border officials and relevant national agencies, reflecting a multi-actor coordination model in border governance (Lutfie & Suharjimantoro, 2025). However, broader cyber incidents are addressed within each country's national cybersecurity framework, where policies emphasize incident response capabilities and cross-sectoral coordination (Oyadeyi et al., 2024).

Publicly available literature does not indicate the existence of specific bilateral cyber incident protocols at many border crossings, reflecting a broader gap in cross-border cybersecurity coordination (Albaheth, 2025; Shaikh et al., 2026). Various studies consistently highlight that the absence of standardized incident response procedures can lead to delays, miscommunication, and reliance on ad hoc mechanisms among national authorities (Ndubuisi, 2022). In the context of Skouw–Wutung, this suggests that institutional alignment does not automatically translate to effective cyber coordination, as response mechanisms remain embedded within a fragmented national framework rather than within a formally structured bilateral arrangement (Adeyeri & Abroshan, 2024).

The Sota Border Post

The Sota Integrated Border Post in Merauke is one of the strategic entry points along the Indonesia–Papua New Guinea border and forms part of Indonesia's broader efforts to modernize and develop its border infrastructure. Various studies describe Sota as a relatively modern and integrated facility, equipped with administrative and public service functions that support cross-border mobility and local economic activities (Metherall et al., 2022; Pugu & Pusung, 2025). Similar to other Indonesian border posts, Sota is embedded within a broader border governance system that increasingly relies on interconnected administrative and digital infrastructure to manage immigration, customs, and security

processes (Adeyeri & Abroshan, 2024). However, despite these similarities, its institutional arrangements differ significantly from those of more established border crossings.

Unlike Skouw, Sota operates within a more asymmetrical institutional environment, as it does not yet have a fully developed or formally institutionalized counterpart border post on the Papua New Guinea side. Existing studies on the Sota–PNG border highlight that cross-border interactions in this region remain unstructured and are often mediated through indirect or higher-level government mechanisms, rather than through directly paired local institutions (Metherall et al., 2022; Pugu & Pusung, 2025). This situation reflects a broader pattern of asymmetry in Indonesia–PNG border governance, where disparities in infrastructure development and institutional capacity shape the nature of cross-border coordination (Darmastuti et al., 2026). Consequently, communication—especially during disruptions—tends to rely more heavily on Indonesian authorities and formal diplomatic channels.

This asymmetry has important analytical implications. The literature on border governance indicates that imbalanced institutional arrangements can affect the speed of communication, clarity of roles, and effectiveness of coordinated responses, particularly in situations involving technical or cross-sectoral disruptions (Adeyeri & Abroshan, 2024; Moniz, 2025). In the case of Sota, the absence of an official counterpart increases the likelihood that technical issues, such as disruptions to digital or cyber systems could escalate into broader coordination challenges. As a result, response efforts are more likely to rely on national-level agencies rather than direct bilateral mechanisms at the border itself, making Sota analytically distinct from more symmetrical crossings like Skouw.

Comparative Implication

Overall, a comparison between Skouw–Wutung and Sota reveals that the Indonesia–Papua New Guinea border is institutionally asymmetrical, with varying configurations of cross-border coordination capacity. Skouw benefits from having direct counterpart agencies, enabling faster interaction between border authorities, while Sota operates without such institutional symmetry. This difference is significant because the management of cyber incidents at digitized border posts depends not only on technical infrastructure but also on the availability of institutional relationships, communication channels, and coordinated response mechanisms. Recent studies on border governance and cybersecurity emphasize that gaps in institutional arrangements, particularly across jurisdictions can hinder coordination and complicate incident response (Adeyeri & Abroshan, 2024; Wallis et al., 2025). Therefore, the asymmetry between Skouw and Sota supports the argument that border cybersecurity vulnerabilities are influenced not only by technical risk exposure but also by an uneven institutional environment and varying coordination capacities.

This institutional comparison also helps explain why asymmetric securitization is particularly relevant in the Indonesia–Papua New Guinea context. Differences in national

cybersecurity capabilities and governance frameworks shape how each country perceives and prioritizes cyber threats. Indonesia has developed a more comprehensive cybersecurity governance architecture and has faced significant national-level cyber disruptions in recent years, leading to a stronger emphasis on incident response and coordinated crisis management (Raditio, & Choiruzzad, 2024). In contrast, Papua New Guinea remains in the early stages of digital and cybersecurity development, with ongoing efforts focused on building regulatory frameworks, institutional capacity, and basic infrastructure (Natanegara et al., 2023). This disparity reflects a broader pattern of asymmetric state capacities in the Pacific Island nations, where differences in institutional development affect security coordination and the effectiveness of responses (Oppenheimer, 2023; Wallis et al., 2025). Consequently, these differences are not merely technical but also interpretive, influencing how cyber risks at the borders are understood, prioritized, and securitized by each country.

Securitization Dynamics and Asymmetric Threat Perception

Cyber threats at borders are not solely technical problems; they are also shaped by socio-political processes through which states define, communicate, and prioritize threats. Securitization Theory from the Copenhagen School (Buzan, Wæver, and de Wilde) provides a useful framework to explain why institutional gaps may persist and how divergent threat constructions can produce diplomatic risk at the Indonesia–PNG border. This study treats asymmetric securitization as a key explanatory mechanism that links differences in institutional capacity to persistent coordination failures and escalation risks at the Indonesia–Papua New Guinea border.

Securitization refers to the elevation of an issue from the realm of normal politics into the realm of security through speech acts that persuade relevant audiences to accept an existential threat framing, thereby legitimizing extraordinary measures (Buzan et al., 1998; Silva & Pereira, 2024). The process involves interrelated elements: a referent object deemed under threat, securitizing actors with authority to articulate the threat, and an audience whose acceptance is required for securitization to succeed (Karyotis et al., 2025). A key implication is that securitization does not simply reflect objective danger; it reflects how threats are narrated, interpreted, and politicized.

Cyber threats complicate securitization because they are characterized by attribution ambiguity, limited visibility, and impacts that can be framed as either disruptive or existential depending on political interpretation (Arslan, 2024; Dunn, 2014). This ambiguity opens space for contested assessments of severity and urgency. Moreover, cyber security often exhibits "double securitization" dynamics: technical communities focus on vulnerabilities and risk management, while political actors frame cyber threats as strategic instruments within broader power competition (Buchanan, 2017). The disjuncture between technical and political framing can create uneven perceptions about what counts as proportional response.

Against this backdrop, differences in institutional capacity and technical expertise between Indonesia and PNG generate conditions for asymmetric securitization (Mahroza et al., 2022). Indonesia, with a more established institutional ecosystem (including BSSN (National Cyber and Crypto Agency), greater technical capacity, and stronger security-sector involvement, may be more inclined to securitize cyber threats at the border as high-stakes security issues requiring extraordinary measures (Wibowo et al., 2024). Papua New Guinea, meanwhile, faces a different policy environment, cyber governance institutions such as DICT (Department of Information and Communications Technology**)** and the implementation of its national strategy are comparatively newer, and official attention often remains concentrated on development priorities and capacity-building (Kia, 2024). The result is a structural mismatch in perceived urgency, resource allocation, and expectations for response. By foregrounding asymmetric securitization, the analysis shows that the problem is not merely uneven capacity, but the absence of a shared security framing that would make bilateral cyber cooperation politically feasible.

This asymmetry is not only a coordination problem, but it can also feed into security dilemma dynamics. Classic security dilemma logic suggests that measures taken defensively by one side may be interpreted as threatening by the other, thereby increasing mutual insecurity (Jervis, 1978). Cyber scholarship similarly highlights that defensive monitoring or intrusion detection activities can be misread as offensive preparation, accelerating mistrust (Buchanan, 2017). In a border context, if Indonesia expands surveillance or cyber defense posturing in ways PNG interprets as intrusive or militarized, a spiral of suspicion becomes more likely, especially absent agreed communication and incident management procedures.

From this perspective, institutional gaps, such as the absence of bilateral protocols and shared attribution mechanisms, are not merely administrative oversights, they are outcomes that become harder to correct when threat perceptions remain misaligned. Bilateral frameworks are typically more feasible when both sides share a baseline understanding of urgency and proportionality. Where Indonesia frames cyber cooperation as part of a broader security architecture while PNG frames it primarily as capacity-building, bargaining preferences and acceptable commitments may diverge (Marles et al., 2025). This divergence contributes to a persistent policy gap at precisely the moment when digitized border operations increase mutual exposure.

Identity, Norms, and the Absence of Common Understanding

This section argues that beyond asymmetric securitization, differences in state identity and the absence of shared norms play a central role in preventing effective cybersecurity cooperation between Indonesia and Papua New Guinea. While securitization theory explains how cyber threats become security issues, constructivism highlights how identities, norms, and shared understandings shape the prospects for cooperation (Sjoberg et al., 2019). In the Indonesia–PNG border context, institutional gaps are reinforced not only by

asymmetric securitization but also by the lack of a common interpretive framework regarding what constitutes a cyber threat, what responses are legitimate, and what constitutes escalation (Aria, 2025).

Constructivist analysis foreground's identity, such as, how states understand who they are and what roles they occupy in specific issue domains (Grzybowski, 2019). Indonesia's identity construction in cybersecurity tends to emphasize institutional maturity and leadership, supported by the presence of BSSN and more extensive technical and security-sector involvement (Mahroza et al., 2022). The PDNS (Temporary National Data Centre) ransomware incident, and the intensity of the subsequent response, further reinforced an identity of high sensitivity to cyber governance risks, even while exposing vulnerabilities (Wibowo et al., 2024). PNG, by contrast, is still consolidating its cyber governance architecture; its national strategy has entered implementation relatively recently, and its position remains shaped by longstanding relationships with partners such as Australia and the country's growing Indo-Pacific strategic salience (Marles et al., 2025). This tends to position PNG as a recipient of capacity support rather than an equal co-designer of frameworks.

Such identity asymmetry complicates partnership design. When one side frames itself as a leader/mentor and the other perceives participation as potentially subordinate, agreements can become politically sensitive and less attractive, even if the technical need is clear (ASEAN, 2024; Habibie et al., 2025). In practice, this reduces incentives to commit to binding protocols and may contribute to the persistence of informal, ad hoc coordination.

The absence of shared norms on cyber incident response is especially consequential. International cyber norms are emerging but remain unevenly consolidated (Rosert, 2024). At the bilateral level, the lack of shared expectations produces three risks. First, the same incident may be interpreted through different doctrinal lenses, Indonesia may draw on evolving international norms and broader strategic cyber doctrines, while PNG may rely more on localized practices or partner-based guidance. Second, without shared norms or procedures for attribution, technical uncertainty becomes politically dangerous, disagreement over responsibility can escalate suspicion. Third, without norms clarifying what actions are escalatory versus proportional, crisis behavior becomes more unpredictable, increasing the chance of retaliatory or symbolic responses that intensify the security dilemma.

Trust, in constructivist terms, develops through repeated interaction, communication, and identity alignment. In the Indonesia–PNG relationship, historical frictions around migration, boundaries, and resource issues can predispose both sides toward cautious interpretation of each other's actions (De Mattos et al., 2025). In a cyber incident, this background can accelerate worst-case assumptions. For example, Indonesia may treat PNG's vulnerabilities as third-party exploitation risks and propose measures that PNG experiences

as intrusive; conversely, PNG may interpret Indonesia's investments as a sign of offensive intent (Kello, 2017).

Despite these constraints, constructivism also suggests pathways for norm-building through dialogue, negotiation, and repeated interaction (Kaneko, 2024). Norm entrepreneurship and gradual internalization can occur via sustained bilateral engagement involving policymakers, technical experts, and security professionals (CIRIS, 2024). However, for norm-building to be viable, the process must be framed carefully, if it appears as an extension of major-power alignment dynamics, it risks undermining bilateral trust. Given the broader geopolitical context, including shifting security dynamics in the Indo-Pacific, bilateral efforts should be explicitly positioned as practical cooperation driven by shared border exposure rather than as part of external strategic alignment.

Escalation Mechanisms and Regional Implications

The preceding analysis indicates that cyber incidents affecting Indonesia–PNG border infrastructure cannot be treated as purely technical disruptions. Under conditions of institutional fragility and asymmetric threat framing, technical incidents can escalate into diplomatic crises, with spillovers into regional stability and broader Indo-Pacific security competition (Radu, 2025).

A first escalation pathway involves ransomware attacks on border-critical systems such as immigration databases or customs payment platforms. Ransomware is increasingly treated as a major national security concern for critical infrastructure (Communications Security Establishment Canada, 2024). In a crisis scenario, the escalation begins with attribution uncertainty. Both governments would likely launch parallel investigations, but the lack of joint technical information-sharing would make conclusions diverge (FP Analytics, 2025). Divergence in attribution can then move quickly into mutual accusation, particularly if one side frames the incident as evidence of irresponsible state behavior or a permissive environment for cybercriminals. Under asymmetric securitization, Indonesian statements emphasizing "alarming vulnerabilities" on the PNG side could be read as insinuations of negligence or complicity, prompting defensive reactions. A subsequent stage involves security dilemma dynamics: heightened monitoring or defensive cyber measures can be interpreted as offensive penetration attempts, encouraging PNG to seek external assistance, including from Australia, which further complicates bilateral relations (FP Analytics, 2025).

A second escalation mechanism involves a data breach affecting an integrated immigration dataset that includes personal information of border residents from both countries. The first stage is contestation over responsibility is each side may blame the other's weak controls, encryption practices, or insider risks (Radu, 2025). Without forensic cooperation frameworks, objective joint investigation becomes difficult, and public communication may quickly politicize the dispute. Media narratives can amplify

reputational frames (e.g., "unreliable partner" versus "unfair blame"), generating domestic pressure for assertive responses. The human impact can further deepen mistrust, such as affected communities may face harassment, discrimination, or heightened inter-group tensions, which can embed conflict into social relations at the border (Zhang et al., 2025).

A third pathway involves coincidence cyber and physical incidents (e.g., smuggling disputes or demarcation tensions). When digital disruptions occur alongside physical events, both sides may interpret them as coordinated hostile actions rather than independent incidents. This compresses decision time, intensifies worst-case assumptions, and increases the likelihood of rapid escalation.

The regional implications are substantial. Escalation could draw in external actors, particularly Australia, given its strategic interests in Pacific stability and capacity-building roles (Marles et al., 2025). In an Indo-Pacific competition context, heightened Indonesia–PNG tension could also become an entry point for broader influence-seeking by major powers, potentially polarizing alignments and complicating crisis management (Fixler, 2025). Further spillovers may affect ASEAN dynamics if tensions become politicized within regional forums, weakening collective cybersecurity confidence-building efforts (ASEAN, 2025). Finally, operational disruption at border posts could produce humanitarian and socio-economic impacts by interrupting trade and people-to-people contact in already constrained border communities (Joshi et al., 2025).

These risks reinforce the policy urgency of developing explicit bilateral cyber cooperation mechanisms, agreed incident response protocols, joint attribution and forensic cooperation arrangements, and confidence-building measures to reduce misinterpretation and manage escalation. Without such institutionalization, technical incidents are more likely to become political crises as digital dependence on border sites deepens.

CONCLUSION

This study demonstrates that cybersecurity vulnerabilities at the Indonesia–Papua New Guinea border are not merely technical issues but are closely intertwined with institutional gaps and asymmetric threat perceptions that can undermine diplomatic stability. By applying securitization theory and constructivism, the analysis shows that cyber incidents at border infrastructure become politically consequential when the two states interpret the same risks with different levels of urgency, responsibility, and proportionality.

The findings highlight three key points. First, the absence of a bilateral cybersecurity framework at the Skouw and Sota border crossing points leaves both countries vulnerable to miscoordination during cyber incidents, especially given the vertical dependence of border systems on national digital infrastructure. Second, asymmetric securitization reinforces these institutional weaknesses: Indonesia tends to frame cyber threats as high-priority security issues requiring extraordinary responses, while Papua New Guinea approaches them primarily as technical and developmental challenges. This divergence complicates

cooperation and increases the likelihood that routine cyber incidents escalate into political disputes. Third, historical trust deficits and the lack of shared norms on incident response and attribution further amplify escalation risks, particularly in moments of crisis.

Several lessons emerge from this analysis for improving awareness of cyberattacks in the Indonesia–PNG border region. Awareness should extend beyond technical detection to include shared understanding of how cyber incidents are interpreted and politicized across borders. Without common expectations regarding proportional response and communication, cyber incidents are likely to generate suspicion and diplomatic friction. Strengthening awareness therefore requires institutionalized dialogue, transparency, and joint preparedness rather than unilateral defensive measures. Establishing a bilateral framework for border cybersecurity, supported by confidence-building measures and regular coordination, would not only enhance cyber resilience but also reduce the risk of escalation in an increasingly digitized and geopolitically sensitive border environment.

REFERENCES

Abrar, A. N. (2021). The role of collaborative journalism in westpapua a jubi and tirto case study. *Pacific Journalism Review*, *27*(1–2), 119–131. https://doi.org/10.24135/pjr.v27i1and2.1174

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*. https://doi.org/https://doi.org/10.3390/info15110682

Alaeifar, P., Pal, S., Jadidi, Z., Hussain, M., & Foo, E. (2024). Current approaches and future directions for Cyber Threat Intelligence sharing: A survey. *Journal of Information Security and Applications*, *83*, 103786. https://doi.org/10.1016/j.jisa.2024.103786

Albaheth, H. E. (2025). Cybercrime Risks in Cross-Border Investment Contracts: Legal Challenges and Regulatory Responses in Commercial and Investment Law. *International Journal of Cyber Criminology*, *19*(1), 138–153. https://doi.org/10.5281/zenodo.476619107

Aria, N. (2025). The Power of Ideas: A Constructivist Reinterpretation of Security in International Relations. *Journal of Social Sciences and Humanities*, *2*(3), 18–36. https://doi.org/10.62810/jssh.v2i3.120

Arslan, A. S. (2024). Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study. *APSA Preprints*. https://doi.org/https://doi.org/10.33774/apsa-2023-wvw2z-v6

ASEAN. (2025). *ASEAN-IPR Regional Conference on Cybersecurity and the Role of Information Technology in Fostering a Culture of Peace in ASEAN*. ASEAN Institute for Peace and Reconciliation (ASEAN-IPR). https://asean-aipr.org/activities/conferences/asean-ipr-regional-conference-on-cybersecurity-and-the-role-of-information-technology-in-fostering-a-culture-of-peace-in-asean

ASEAN. (2024). *Blue Book 2024: European Union and the Association of Southeast Asian Nations*

(EU–ASEAN Partnership).

Asemki, Y., Nurmandi, A., & Muallidin, I. (2023). The Dynamics of Cyber-Activists in the Digital Era of Papua, Indonesia. *Lecture Notes in Networks and Systems*, *464*, 377–388. https://doi.org/10.1007/978-981-19-2394-4_35

Berawi, M. A., Miraj, P., & Sidqi, H. (2017). Plastic degrading fungi Trichoderma viride and Aspergillus nomius isolated from Nouban, F. and Abazid, M. (2017) 'Plastic degrading fungi Trichoderma viride and Aspergillus nomius isolated from local landfill soil in Medan', Iopscience.Iop.Org,. *Iopscience.Iop.Org*, *8*(February 2018), 68–74.

Bowen, G. A. (2017). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2). https://doi.org/10.46743/2160-3715/1992.2039

Braun, V., & Clarke, V. (2021). Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. *Counselling and psychotherapy research*, *21*(1), 37-47.

Buchanan, B. (2017). *The Cybersecurity Dilemma: Where Thucydides Meets Cyberspace*. Council on Foreign Relations Blog. https://www.cfr.org/blog/cybersecurity-dilemma-where-thucydides-meets-cyberspace

Buchkovska, K. (2025). Cyber Diplomacy: Securing the (Digital) Future. *Journal of Law and Politics*, *6*(1), 97–108. https://doi.org/10.69648/qpko3766

Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity. From threat detection to policy learning. *Government Information Quarterly*, *42*(1), 102000. https://doi.org/10.1016/j.giq.2024.102000

Buzan, B., Wæver, O., & Wilde, J. de. (1998). Security: A New Framework for Analysis. In *ペインクリニック学会治療指針２* (First Edit). Lynne Rienner Publishers.

CCB. (2021). *Cybersecurity Strategy Belgium 2.0 2021-2025* (Issue May 2021). https://share.google/CsZKFy8Ai0kA9cJnZ

Central Bureau of Statistics of Papua Province. (2025). *Perkembangan Ekspor dan Impor Provinsi Papua, Mei 2025*. https://papua.bps.go.id/id/pressrelease/2025/07/01/1154/perkembangan-ekspor-dan-impor-provinsi-papua--mei-2025.html?utm_source=

Chaudhuri, A., Sarkar, S., & Bala, P. K. (2025). Thematic Exploration and Analysis of Cybersecurity Policies of Businesses: An NLP-Based Approach. *Journal of Organizational Computing and Electronic Commerce*, *35*(2), 157–187. https://doi.org/10.1080/10919392.2024.2435115

CIRIS. (2024). *Norm Cascade in International Relations*. CIRIS Learning Center. https://www.ciris.info/learningcenter/norm-cascade-in-international-relations/

Communications Security Establishment Canada. (2024). *National Cyber Threat Assessment 2025-2026*.

Costa, G. Da. (2024). *Indonesia, Papua New Guinea strengthen defense ties with training, border*

security initiatives. IP Defense Forum. https://ipdefenseforum.com/2024/08/indonesia-papua-new-guinea-strengthen-defense-ties-with-training-border-security-initiatives/

Darmastuti, S., Nidatya, N., Saraswati, D. P., & Rahmalia, A. N. (2026). Political Economy of Cross-Border Trade Between Indonesia and Malaysia: Local Product Opportunities and Challenges in West Kalimantan. *JWP (Jurnal Wacana Politik)*, *11*(1), 1-14.

De Mattos, C., Salciuviene, L., & Sanderson, S. (2025). Can conflict be a desirable step in trust-building within international strategic alliances? A systematic literature review and typology: Positive employment of conflicts in alliances. *Journal of International Management*, *31*(2), 1-36. https://doi.org/10.1016/j.intman.2025.101234

Dept of Information & Communication Technology. (2023). *National Cyber Security Strategy 2024 – 2030*. Department of Information & Communications Technology, Papua New Guinea. https://www.ict.gov.pg/ncss/

Dunn, C. M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

Fixler, A. (2025, April 29). *Shaping the Future of Cyber Diplomacy: Review for State Department Reauthorization – Written Testimony*. https://www.fdd.org/analysis/2025/04/29/shaping-the-future-of-cyber-diplomacy/

FP Analytics. (2025). *Ransomware Rising: Confronting the fastest-growing cybercrime through international cooperation*. Digital Front Lines (Sub-Site Dari FP Analytics). https://digitalfrontlines.io/2025/09/03/ransomware-rising/

Grzybowski, J. (2019). The paradox of state identification: De facto states, recognition, and the (re-)production of the international. *International Theory*, *11*(3), 241–263. https://doi.org/10.1017/S1752971919000113

Gunawan, B., Nurisnaeny, P. S., Kaprisma, H., & Ratmono, B. M. (2024). Border Security in Intelligence Perspective: A Bibliometric Analysis (1985-2022). *Proceedings of the International Seminar on Border Region (INTSOB 2023)*, *Intsob 2023*, 28–38. https://doi.org/10.2991/978-2-38476-208-8_6

Habibie, S. Y., Rudiyanto, & Said, B. D. (2025). Navigating Asymmetric Interdependence: s Neoliberal Institutionalist Perspective on ASEAN-China Ties. *International Journal of Progressive Sciences and Technologies (IJPSAT)*, *49*(1), 1–10.

Harefa, F., & Supriyadi, A. A. (2025). Leadership strategies for enhancing border security in Papua: A collaborative approach to surveillance and threat management. *Journal of National Paradigm-Based Resilience Strategy*, *2*(1), 1–16. https://doi.org/https://doi.org/10.61511/napbres.v2i1.2025.1731

Hutagalung, S. (2024, December 20). *Asia-Pacific At A Crossroads: Addressing Conflict In Key Geopolitical Hotspots – Analysis*. Eurasia Review. https://www.eurasiareview.com/20122024-asia-pacific-at-a-crossroads-addressing-conflict-in-key-geopolitical-hotspots-analysis/

Jervis, R. (1978). Cooperation Under the Security Dilemma. *World Politics*, *20*(2), 167–214. https://doi.org/https://doi.org/10.2307/2009958

Johnson, B., & Ziogas, A. (2024, December 11). Instability in Pacific politics? Yes, but it's stable instability. *The Strategist (Australian Strategic Policy Institute)*. https://www.aspistrategist.org.au/instability-in-pacific-politics-yes-but-its-stable-instability/

Joshi, A., Moschetta, G., Winslow, E., Buys, W., & Herrmann, A. (2025). *Global Cybersecurity Outlook 2025* (Issue January).

Kaifa, U., Yaseen, D. Z., & Muzaffar, D. M. (2025). A thematic analysis of Pakistan's cybersecurity policies, regulations and implications. *Journal of Climate and Community Development*, *4*(1), 39-54.

Kaneko, J. (2024). What constitutes bilateral intergovernmental technical cooperation in the financial-sector?: towards the development of a systematic methodology. *Cogent Social Sciences*, *10*(1). https://doi.org/10.1080/23311886.2024.2404686

Karyotis, G., Paterson, I., & Judge, A. (2025). Understanding Securitization Success: A New Analytical Framework. *International Studies Review*, *27*(1). https://doi.org/10.1093/isr/viaf006

Kello, L. (2017). *The Security Dilemma of Cyberspace: Ancient Logic, New Problems*. Lawfare (Lawfare Institute). https://www.lawfaremedia.org/article/security-dilemma-cyberspace-ancient-logic-new-problems

Kia, L. (2024). *Papua New Guinea Makes Major Leap in Global Cybersecurity Rankings*. Department of Information and Communications Technology, Papua New Guinea. https://www.ict.gov.pg/22922/

Korwa, J., & Rumabar, B. (2024). *Challenges ahead for Indonesia-PNG cross-border cooperation*. Devpolicy Blog, Development Policy Centre. https://devpolicy.org/challenges-ahead-for-indonesia-png-cross-border-cooperation-20240918/?utm_source=chatgpt.com

Lutfie, R. Z., & Suharjimantoro, S. (2025). Political Dynamics And Policy Implications Of Indonesia-Australia Border Management. *JWP (Jurnal Wacana Politik)*, *10*(1). https://doi.org/https://doi.org/10.24198/jwp.v10i1.59186

Mahroza, S., Priyanto, & Halkisy, M. (2022). Asymmetric Diplomacy and Securitization in The South China Sea. *Andalas Journal of International Studies*, *11*(1), 94–107. https://doi.org/https://doi.org/10.25077/ajis.11.1.94-107.2022

Marles, R., Wong, P., Sugiono, & Sjamsoeddin, S. (2025, August 28). *Joint Statement on the Ninth Australia-Indonesia Foreign and Defence Ministers' 2+2 Meeting*. Department of Defence, Australia. https://www.minister.defence.gov.au/statements/2025-08-28/joint-statement-ninth-australia-indonesia-foreign-defence-ministers-22-meeting

Metherall, N., Fretes, D. R. De, Mandibondibo, F., & Caucau, T. (2022). Assessing the Development Impact of the Sota Border Post Connecting Indonesia and Papua New Guinea. *Papua Journal of Diplomacy and International Relations*, *2*(2).

https://doi.org/10.31957/pjdir.v2i2.2209

Moniz, E. de A. (2025). The Journal of Academic Science Cybersecurity Governance in ASEAN: Building a Regional Cyber-Emergency Response Framework. *The Journal of Academic Science*, *2*(11), 2356–2366.

Natanegara, A. H., Budiman, L., & Nidhal, M. (2023). Understanding the regulatory environment for ICT infrastructure in Papua New Guinea. *Center for Indonesian Policy Studies*, *16*.

Ndubuisi, A. F. (2022). Cross-border jurisdiction challenges in prosecuting cybercrime syndicates targeting national financial and electoral systems. *International Journal of Engineering Technology Research & Management*, *6*(11), 243–261.

Nugroho, Y. (2024, August 8). *Indonesia's National Data Centre Ransomware Attack: A Digital Governance Failure?* Iseas Yusof Ishak Institute. https://fulcrum.sg/indonesias-national-data-centre-ransomware-attack-a-digital-governance-failure/

Nurisnaeny, P. S., Mubaroq, S. R., Kaprisma, H., Perdana, I. A., & Budiman, R. (2025). Developing an AI-Enhanced Maritime Border Security Framework: A Case Study of Indonesia-Malaysia Border at Sebatik Island. *Sosiohumaniora*, *26*(3), 453–467. https://doi.org/10.24198/sosiohumaniora.v26i3.60820

Oppenheimer, H. (2023). *The Failed Digital State Problem? Capacity Gaps and Managing Internet Externalities*. https://share.google/inUHGQjjbwwLbOoIy

Oyadeyi, O. O., Oyadeyi, O. A., & Bello, R. O. (2024). Cybercrime in the Asia-Pacific Region : A Case Study of Commonwealth APAC Countries. *Commonwealth Cyber Journal*, *June*, *130-160*.

Praditya, E., Maarif, S., Ali, Y., Saragih, H. J. R., Duarte, R., Suprapto, F. A., & Nugroho, R. (2023). National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence. *Journal of Human Security*, *19*(2), 91–106.

Pugu, M. R., Yani, Y. M., & Wardhana, W. (2019). Pembangunan Infrastruktur Di Perbatasan Papua: Upaya Menjamin Human Security Dan Melawan Perdagangan Illegal Lintas Batas. *Masyarakat Indonesia*, *45*(1), 76-92.

Pugu, M. R., & Pusung, M. (2025). Socio-Economic Dynamics at the Border: A Case Study of the Sota, Merauke Cross-Border Post and Its Implications for Cooperation with Papua New Guinea. *Journal of Social Research*, *4*(10), 2637–2647. https://doi.org/https://doi.org/10.55324/josr.v4i9.2782

Putra, M. E. (2022). Review of the Internet Blocking Case in Papua in Cyber Law Perspective. *Lampung Journal of International Law*, *4*(1), 47–52. https://doi.org/10.25041/lajil.v4i1.2524

Raditio, K.H., & Choiruzzad. (2024). *Dynamics in the Indo-Pacific: From Geopolitics and Geoeconomics Perspectives (Eds).* The Habibie Center (THC). https://share.google/j78Lm6qcuar85SH93

Radu, R. (2025). Countering Ransomware: Government Responses in a Comparative Perspective. *International Conference on Cyber Conflict, CYCON*, *14333*, 91–108.

https://doi.org/10.23919/CyCon65856.2025.11103717

Rainforest Rescue. (2025, August 7). *Indonesia: The future of Papua hangs in the balance*. Rainforest Rescue. https://www.rainforest-rescue.org/updates/14119/indonesia-the-future-of-papua-hangs-in-the-balance

Robinson, R. (2024, June 21). Cyber Diplomacy: A New Frontier in International Relations and Professional Practice. *ComplexDiscovery*. https://complexdiscovery.com/cyber-diplomacy-a-new-frontier-in-international-relations-and-professional-practice/

Rosert, E. (2024). Effects of international norms: A typology. *Journal of International Political Theory*, *20*(1), 22–40. https://doi.org/10.1177/17550882231184275

Rupp, C., & Paulus, A. (2023). *Official Public Political Attribution of Cyber Operations* (Issue October).

Shaikh, R. K., Anjum, R., & Barkat, A. (2026). Cyber-Security Beyond Borders: Unraveling Cross-Jurisdictional Legal Complexities in Cyberspace. *Advance Social Science Archive Journal*, *05*(01), 334–352. https://doi.org/https://doi.org/10.5281/zenodo.18301634

Silva, C. C. V., & Pereira, A. E. (2024). Securitization theory and its empirical application: a literature review. *Revista de Sociologia e Politica*, *32*, 1-22. https://doi.org/10.1590/1678-98732432e019

Sjoberg, L., Constructivist, S. D., Approaches, C., Barkin, J. S., & Sjoberg, L. (2019). Book review: J. Samuel Barkin, Laura Sjoberg, International Relations' Last Synthesis? Decoupling Constructivist and Critical Approaches, New York 2019, pp. 224. *Polish Political Science Yearbook*, *48*(2), 375–376. https://doi.org/https://doi.org/10.15804/ppsy2019212

Souisa, H., & Renaldi, E. (2025, October 9). Indonesia urges respect for its sovereignty after Australia-PNG defence treaty. *ABC News*. https://www.abc.net.au/news/2025-10-10/indonesia-responded-pukpuk-defence-agreement-australia-png/105869738

Sumadinata, R. W. S., Achmad, W., & Riyadi, S. F. (2022). Indonesian Border Defense Policy: A Case Study on the Interoperability of the joint regional defense command. *Central European Management Journal*, *30*, 886–895.

The European Union Agency for Cybersecurity. (2024). *Best practices for cyber crisis management* (Issue February). https://op.europa.eu/publication/manifestation_identifier/PUB_TP0523461ENN

The U.S. Intelligence Community. (2025). *Annual Threat Assessment of the U.S. Intelligence Community 2025* (Issue March). https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

Thumfart, J. (2022). The (Il)legitimacy of Cybersecurity. An Application of Just Securitization Theory to Cybersecurity based on the Principle of Subsidiarity. *Applied Cybersecurity and Internet Governance*, *1*(1), 1–24. https://doi.org/10.5604/01.3001.0016.1093

Wallis, J., McNeill, H., Batley, J., & Powles, A. (2025). *Security Cooperation in the Pacific Islands*

(J. Wallis, H. McNeill, J. Batley, & A. Powles (eds.)). Routledge.

Wendt, A. (1995). Constructing international politics. *International security, 20*(1), 71-81.

Wibowo, S. E., Hartono, A., Kiswanto, H., Primawanti, H., & Louerens, J. T. A. (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.v8i2.13817

Wickham, D. (2025, May 2). *Manele under threat: the political crisis in Solomon Islands*. Devpolicy Blog, Development Policy Centre. https://devpolicy.org/manele-under-threat-the-political-crisis-in-solomon-islands-20250502/

Yuniar, A. (2025, September 8). *Collaboration is the key to Indonesia cyber resilience: BSSN*. GovInsider Asia. https://govinsider.asia/intl-en/article/collaboration-is-the-key-to-indonesia-cyber-resilience-bssn

Zhang, H., Yang, C., Deng, X., & Luo, C. (2025). How Authoritative Media and Personal Social Media Influence Policy Compliance Through Trust in Government and Risk Perception: Quantitative Cross-Sectional Survey Study. *Journal of Medical Internet Research*, *27*, 1–16. https://doi.org/10.2196/64940

ABOUT THE AUTHORS

Dewi Anjani Kartika Putri is a Master's student in the International Relations Postgraduate Program at Universitas Muhammadiyah Yogyakarta, Indonesia, where she earned her bachelor's degree in International Relations. Her research interests include cybersecurity and institutional vulnerabilities, conflict and diplomatic crises in international relations, and digital diplomacy.

Ali Maksum is the Secretary of the International Relations Master's Program (HIPM) at Universitas Muhammadiyah Yogyakarta, Indonesia, and a lecturer in International Relations. He is also the principal of the Malindo Nusantara Research Centre. His research focuses on Indonesian foreign policy, migration, and Southeast Asian studies.

HOW TO CITE THIS ARTICLE:

Putri, D.A.K., & Maksum, A. (2026). Cybersecurity Vulnerabilities at the Indonesia–Papua New Guinea Border: Securitization Asymmetry, Institutional Gaps, and Diplomatic Escalation. *Papua Journal of Diplomacy and International Relations, 6*(1), 43-67. DOI: 10.31957/pjdir.v6i1.5041