Indonesia–Japan Cooperation in Countering Cyberterrorism and Strengthening Cyber Resilience: Toward Legal–Institutional Convergence

Eko Setyo Utomo[1] , Eva Achjani Zulfa[2], Solikhah Yuliatiningtyas[3] , and M. Syaroni Rofi'i[4]

[1] School of Strategic and Global Studies, Universitas Indonesia, Depok 16424-Indonesia
[2] School of Strategic and Global Studies, Universitas Indonesia, Depok 16424-Indonesia
[3] School of Strategic and Global Studies, Universitas Indonesia, Depok 16424-Indonesia
[4] School of Strategic and Global Studies, Universitas Indonesia, Depok 16424-Indonesia
Corresponding author: eko.setyo21@ui.ac.id

Abstract. The convergence of cyberterrorism, artificial intelligence (AI), and hybrid warfare presents multidimensional challenges to national security and regional stability. This article analyzes Indonesia–Japan cooperation in countering cyberterrorism and strengthening cyber resilience, focusing on governance, law, technology, and public–private partnerships. It draws on comparative case study methodology, elite interviews, survey findings, and document analysis. Particular attention is given to Indonesia's draft Cybersecurity and Resilience Bill (RUU KKS), which represents a turning point in the securitization of cyberspace by embedding AI risk governance, critical infrastructure protection, and structured public–private partnerships. Japan's Cybersecurity Basic Act offers a consolidated model for resilience and regional leadership. The article concludes that bilateral cooperation can serve as a replicable model for ASEAN by integrating legal harmonization, AI-powered early warning systems, and institutionalized partnerships.

Keywords: Artificial Intelligence, Hybrid Warfare, Indonesia, Japan, Cybersecurity Policy, RUU KKS, ASEAN

1 Introduction

Indonesia, the world's fourth most populous country and the largest digital economy in Southeast Asia, is increasingly vulnerable to escalating cyber threats with the potential to evolve into cyberterrorism. In 2022 alone, the National Cyber and Crypto Agency (BSSN) reported over 361 million cyberattacks, including malware, phishing, and ransomware, targeting both public and private sectors [17]. These persistent incidents highlight systemic fragilities in critical infrastructures—energy, finance, transportation—that are attractive to both state and non-state actors.

I. S. Fitrinitia et al. (eds.), *Proceedings of the 9th International Conference on Strategic and Global Studies 2025 (ICSGS 2025)*, Atlantis Highlights in Social Sciences, Education and Humanities 43,
https://doi.org/10.2991/978-94-6463-918-6_13

Recent cases illustrate the blurred line between cybercrime and politically motivated cyberterrorism. The hacker collective Bjorka in 2022 leaked sensitive personal data of Indonesian citizens and officials, undermining public trust in state digital governance [17]. While not classified as terrorism, such incidents demonstrate how cyber intrusions can destabilize governance and erode legitimacy. Analysts further warn that extremist groups—including remnants of Jemaah Islamiyah and pro-ISIS networks—are adopting encrypted communication, digital propaganda, and online recruitment, potentially progressing toward cyber sabotage [14,13,26]. These concerns echo global cases, such as attempted cyberattacks on U.S. water facilities and Ukrainian energy grids, where cyber operations have targeted vital infrastructure [14,15].

Indonesia's threat environment is compounded by structural challenges. Governance fragmentation across BSSN, the Ministry of Digital Affairs, the Indonesian National Police (Polri), and the State Intelligence Agency (BIN) has produced overlapping mandates and unclear authority lines [4,13]. Legal frameworks—including the Information and Electronic Transactions Law (UU No. 11/2008, amended by UU No. 19/2016) [22,23], the Anti-Terrorism Law (UU No. 5/2018) [24], and the draft Cybersecurity and Resilience Bill (RUU KKS) [19]—remain inadequate to address AI-enabled hybrid threats [15,16]. Uneven digital literacy further heightens societal exposure to phishing, disinformation, and radicalization [15,17].

At the regional level, Southeast Asia has emerged as a hotspot for cybercriminal and extremist operations due to weak regulatory frameworks and uneven cybersecurity capacity [15,16]. For Indonesia, this is particularly acute as it advances its Golden Indonesia 2045 digital transformation vision, making cyberinfrastructure simultaneously a strategic asset and a prime target [15,17].

Conceptually, cyberterrorism should not be reduced to isolated technical crime but understood as a multidimensional phenomenon blending political intent, symbolic communication, and technological exploitation [3,7,2,8]. Within the framework of hybrid warfare, it encompasses cyberattacks, disinformation, and psychological operations aimed at eroding public trust and national stability [7,9,10,11]. Artificial intelligence (AI) further magnifies these dynamics through deepfake propaganda, autonomous malware, and adversarial manipulation of algorithms [14,15,15].

By contrast, Japan demonstrates a more consolidated model of cyber resilience. The Cybersecurity Basic Act (Act No. 104/2014, amended 2018) and the leadership of the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) provide legal clarity and centralized coordination, embedding cyber threats into national defence planning [25]. As Balzacq [12] argues, securitization depends on institutional practices and audience acceptance; Japan has effectively institutionalized cybersecurity as an existential national security issue.

These asymmetries frame the contours of Indonesia–Japan cooperation: Japan as a capacity builder, Indonesia as a strategic partner. The draft RUU KKS may serve as a

turning point by consolidating governance, embedding AI risk management, and formalizing public–private partnerships. Situating cyberterrorism within the lenses of hybrid warfare and securitization [2,12,4] enables a nuanced understanding of how bilateral cooperation can advance cyber resilience in the Indo-Pacific.

2 Conceptual Framework and Literature Review

2.1 Defining Cyberterrorism

Cyberterrorism has been the subject of definitional debates since the late 1990s. Denning [3] defines it as the convergence of terrorism and cyberspace, where politically motivated attacks aim to cause fear, disruption, or coercion. Conway [13] emphasizes its dual dimension as both technical and symbolic, arguing that cyberterrorism communicates fear through media amplification as much as it disrupts systems. Weimann [14] highlights the performative nature, suggesting that "the power of fear may outweigh the damage to networks." Jarvis and Macdonald [8] further observe that definitional ambiguity itself has policy consequences, creating uncertainty for legal and institutional responses.

In Indonesia, these definitional ambiguities create a "grey zone of legality," complicating enforcement and weakening deterrence [15]. Legal instruments—including the Information and Electronic Transactions Law (UU No. 11 of 2008, amended by UU No. 19 of 2016) [22,23], the Anti-Terrorism Law (UU No. 5 of 2018) [24], and the draft Cybersecurity and Resilience Bill (RUU KKS) [19]—provide only partial guidance on AI-enabled cyber threats [16]. This lack of clarity makes it difficult to differentiate between cybercrime, cyberterrorism, and hybrid operations, resulting in enforcement challenges and delayed policy responses. Japan, by contrast, adopts a broader and more integrated approach, embedding terrorism-related cyber threats within national cybersecurity frameworks and critical infrastructure protection regimes [25].

2.2 Hybrid Warfare

Hybrid warfare integrates conventional, irregular, informational, and cyber tactics to exploit systemic vulnerabilities. Hoffman [7] conceptualizes hybrid conflict as the blending of kinetic and non-kinetic means, combining conventional military action with subversive, clandestine, or digital operations. Korybko [9] frames hybrid warfare as an adaptive, asymmetric strategy designed to destabilize adversaries across multiple domains simultaneously. Renz and Smith [11] extend this to cyberspace, showing how hybrid strategies leverage both state and non-state capabilities. Mumford [10] highlights the rise of proxy and indirect conflict as part of this broader toolkit.

In Southeast Asia, hybrid methods manifest in the form of coordinated disinformation campaigns, cyber-enabled financial disruption, attacks on critical infrastructure, and information operations targeting public trust. These activities often blur the line between espionage, organized crime, and terrorism, demonstrating that cyberterrorism

is not an isolated phenomenon but an integral component of broader hybrid campaigns. AI-enabled capabilities amplify both offensive and defensive dimensions, creating new challenges in attribution, rapid response, and risk management.

2.3 Securitization of Cyberterrorism

Securitization theory provides a lens to understand how cyberterrorism is framed as an existential threat. According to Buzan et al. [2], an issue becomes a matter of security when it is articulated as a threat to the survival of a referent object—typically the state—legitimizing extraordinary political measures. Balzacq [12] emphasizes that securitization succeeds only when institutional practices and audience acceptance converge, linking discourse with policy outcomes.

Japan illustrates early and coherent securitization, embedding cybersecurity into national defence planning through the Cybersecurity Basic Act [25]. The law provides a clear institutional framework and aligns domestic cyber governance with international standards, facilitating proactive crisis management and resilience-building. Indonesia's securitization has historically been more reactive and fragmented; however, the draft RUU KKS signals a potential breakthrough by elevating cyber threats from technical concerns to strategic national security issues, expanding the mandates of BSSN, and formalizing public–private cooperation [15].

2.4 AI as Threat and Resilience Enabler

Artificial intelligence introduces a dual-use dimension to the cyber threat landscape. Malicious applications—including deepfake propaganda, automated phishing campaigns, and adversarial attacks on machine learning systems—lower the barriers to conducting high-impact cyber operations [14]. At the same time, AI enables enhanced resilience through anomaly detection, predictive analytics, threat intelligence automation, and rapid response systems [15,14]. Dunn Cavelty [4] highlights that political and social narratives shape the deployment and perception of technological risk.

For policy and strategy, AI thus functions both as a multiplier of cyber risks and as a cornerstone of resilience strategies. Integrating AI into cybersecurity governance requires balancing innovation and control, promoting capabilities that detect and respond to threats while mitigating potential abuse. Indonesia's draft RUU KKS reflects this balance by proposing AI oversight mechanisms, but implementation and integration with broader regulatory and institutional frameworks remain nascent [15].

3 Methodology

This study adopts a qualitative comparative case study design to examine Indonesia–Japan cooperation on cyberterrorism and cyber resilience. This approach is particularly suitable for exploring complex and evolving security phenomena at the intersection of

AI, hybrid warfare, and governance [14]. As Yin [28] emphasizes, the case study method enables researchers to capture the holistic and meaningful dynamics of real-life events. By comparing Indonesia with Japan and selected international benchmarks, the research design identifies both context-specific challenges and transferable lessons for policymaking.

3.1 Research Design

The comparative case study method was selected to analyse similarities and differences in governance, legal frameworks, and strategic approaches. This design highlights how two asymmetrical partners—Indonesia as an emerging cyber power and Japan as a technologically advanced state—develop cooperative mechanisms to counter cyberterrorism. The study integrates three methodological components:

- Doctrinal legal analysis, focusing on statutory and regulatory frameworks [22–25,19];
- Empirical fieldwork, including surveys and elite interviews [17,18];
- Secondary literature review, examining scholarly and policy publications [28].

3.2 Data Sources

To ensure robustness and triangulation, data were drawn from multiple sources:

1. **Policy and Legal Documents**: Indonesia's Information and Electronic Transactions Law (UU ITE; Government of Indonesia, 2008/2016) [22,23], Anti-Terrorism Law (Government of Indonesia, 2018) [24], Japan's Cybersecurity Basic Act (Government of Japan, 2014/2018) [25], national cybersecurity strategies, bilateral Memoranda of Cooperation (2018–2024), and the draft RUU Keamanan dan Ketahanan Siber (KKS; DPR RI, 2023) [19].
2. **Institutional Reports**: Publications from Indonesia's National Cyber and Crypto Agency (BSSN) [17], the National Counterterrorism Agency (BNPT) [18], and international organizations including ASEAN [15], UNOCT [26], and Interpol [additional].
3. **Surveys**: An online survey administered in 2025 to 100 Indonesian stakeholders, including policymakers, cybersecurity practitioners, academics, and civil society actors [Author's Survey, 2025].
4. **Elite Interviews**: Conducted between 2024 and 2025 with 15 senior figures from BSSN, BNPT, BIN, Densus 88, DPR RI (Commission I), CSIRT.ID, and academia [Author's Interviews, 2024–2025].

3.3 Analytical Framework

The analysis followed a Grounded Theory–informed approach [4,29,30], which enabled theoretical insights to emerge inductively while being informed by established

frameworks in cybersecurity, securitization, and hybrid warfare. The coding process was iterative, consisting of three stages:

- **Open coding**: identifying initial concepts;
- **Axial coding**: connecting categories;
- **Selective coding**: refining core themes.

Thematic categories included governance and institutional capacity, legal frameworks, AI integration, public–private partnerships (PPPs), and regional/international cooperation. The analysis was guided by the conceptual framework presented in Section 2, drawing on cyberterrorism definitions [3,14,13,8,31], hybrid warfare [7,9,1,additional], securitization [2,12,4,15], and AI/resilience [14,15,additional,additional].

3.4 Reliability, Ethics, and Limitations

Reliability was enhanced through data triangulation (documents, surveys, interviews) and investigator triangulation. Ethical protocols included informed consent, anonymization of interviewees, and compliance with social science standards. Limitations arose from restricted access to intelligence data, limited official reporting, and the nascent stage of Indonesia–Japan bilateral initiatives. These were mitigated through triangulation and situating findings within regional and global contexts [28,26,15].

4 Comparative Analysis: Indonesia and Japan

This section analyses Indonesia–Japan cooperation on cyberterrorism and cyber resilience through five comparative dimensions: governance and institutional architecture, legal frameworks, public–private partnerships (PPPs), intelligence sharing, and technological innovation. These dimensions reveal structural asymmetries that both constrain and enable bilateral collaboration (see **Table 1** for a summary of key comparative indicators between Indonesia and Japan).

4.1 Governance and Institutional Architecture

The governance of cybersecurity in Indonesia and Japan reflects divergent institutional trajectories, shaped by differences in technological maturity, state capacity, and securitization strategies [24,8,15].

- **Indonesia**: Cybersecurity governance in Indonesia remains fragmented despite the establishment of the National Cyber and Crypto Agency (BSSN) in 2017 as the central coordinating body. Overlapping mandates among BSSN, the Ministry of Communication and Digital (Komdigi), the National Police (Polri), and the State Intelligence Agency (BIN) have produced redundancies and blurred lines of authority [15,9,4]. The absence of a unified national

cybersecurity law further complicates coordination, leaving gaps in regulatory enforcement and crisis response [22,23,24]. A senior BSSN official noted: "without a single command structure, cybersecurity incidents risk falling through bureaucratic cracks" [Author's Interview, Jakarta, 2024].

- **Japan**: Japan has developed a centralized and strategic model. The National Centre of Incident Readiness and Strategy for Cybersecurity (NISC), under the Cabinet Secretariat, coordinates across ministries, critical infrastructure operators, and the private sector [25,26,15]. This structure ensures policy coherence and enables Japan to integrate cyberterrorism threats into national security and defence planning. Japan's participation in international regimes—including the Budapest Convention and G7 frameworks—reinforces institutional legitimacy [20,26].

Comparative Insights: Indonesia struggles with fragmentation, whereas Japan benefits from unified governance and strategic framing. This asymmetry provides a foundation for Japan to act as a capacity builder in bilateral cooperation.

4.2 Legal Frameworks

- **Indonesia**: Indonesian law addresses cyber-related offenses primarily through the Information and Electronic Transactions Law (UU ITE, 2008, amended 2016 & 2024) and the Anti-Terrorism Law (UU No. 5/2018) [22,23,24]. These statutes criminalize terrorism and cybercrime separately but lack explicit definitions of cyberterrorism, creating ambiguity when politically motivated attacks occur in cyberspace [11,4]. Indonesia has not ratified the Budapest Convention, limiting normative harmonization with global standards [20]. A BNPT official explained: "our laws criminalize terrorism and cybercrime separately, but cyberterrorism often sits in between, creating legal ambiguity" [Author's Interview, Jakarta, 2024].
- **Japan**: Japan's Cybersecurity Basic Act (2014, revised 2021) links digital security to national defence and economic security [25,15]. Complementary statutes, such as the Unauthorized Computer Access Law (1999) and the Act on the Protection of Personal Information (APPI), regulate specific aspects of cyber activity. Japan's ratification of the Budapest Convention integrates its domestic regime with international law [20]. Yamaguchi [15] observes that Japan's legal architecture "balances sovereignty with a strong outward-looking orientation, embedding international norms into domestic law."

Comparative Insights: Legal asymmetry reflects broader differences in securitization [24,11]. Indonesia's fragmented framework creates ambiguity, while Japan's regime proactively integrates cybersecurity into national defence and international cooperation.

4.3 Public–Private Partnerships (PPPs)

- **Indonesia**: PPPs in Indonesia remain emergent and reactive. BSSN collaborates with telecom providers, banks, and the Association of Internet Service Providers of Indonesia (APJII), but coordination is largely ad hoc [4,11,15]. Limited SME investment, low digital literacy, and weak regulatory incentives reduce effectiveness [9]. A Komdigi policymaker remarked: "the private sector is usually only engaged when there is a major incident, not as part of ongoing structured collaboration" [Author's Interview, Jakarta, 2024].
- **Japan**: Japan institutionalizes PPPs through mechanisms such as J-CSIP and ISACs, which foster systematic collaboration between government, industry, and academia [26,15]. National cyber drills and NICT-led R&D strengthen preparedness and promote innovation [26].

Comparative Insights: Japan's PPPs are proactive, institutionalized, and technologically advanced. Indonesia's remain reactive and episodic. Bilateral cooperation—particularly joint drills, incident reporting protocols, and PPP frameworks—offers opportunities for capacity-building.

4.4 Cyber Intelligence Sharing and Joint Initiatives

- **Indonesia**: Intelligence sharing is fragmented among BIN, BSSN, TNI, and Polri, with siloed data flows and institutional rivalries [15,9,4]. A Densus 88 officer explained: "each agency holds sensitive intelligence, but there is no culture or system of fast, cross-agency sharing" [Author's Interview, 2024].
- **Japan**: NISC coordinates intelligence-sharing across ministries and with the private sector [15]. Japan also engages in structured cooperation with the U.S., EU, and ASEAN, employing AI-based threat detection and early warning systems [26,25].
- **Bilateral Initiatives**: Since 2019, bilateral MoUs have institutionalized cooperation through ASEAN-Japan Cyber Capacity Building Centre (AJCCBC) programs, joint cyber drills, technical exchanges, and the Cyberterrorism Early Warning System (CTEWS) [19,26].

Comparative Insights: Indonesia benefits from Japan's structured approach, while Japan reinforces its regional cybersecurity leadership. Bilateral frameworks provide platforms for bridging Indonesia's intelligence silos.

4.5 Technological Innovation

- **Indonesia**: Indonesia has piloted AI-based anomaly detection and developed cyber ranges, but implementation remains constrained by resource limitations, reliance on foreign vendors, and skill gaps [15,11,9]. As a BSSN official observed: "AI gives us tools to detect anomalies faster, but our challenge is not technology—it's human capital" [Author's Interview, 2024]. Alimurfie [9] similarly notes that "Indonesia's innovation ecosystem is constrained by uneven human capital development."

- **Japan**: Japan is a global leader in emerging technologies, advancing AI, 5G, quantum computing, blockchain, and post-quantum cryptography [26,25,15]. Cyber ranges and predictive analytics are embedded into national strategy, and government–industry–academia collaboration accelerates innovation [26].

Comparative Insights: Innovation gaps highlight structural asymmetry. Japan's advanced ecosystem positions it as a knowledge and technology provider, while Indonesia's resource and skill constraints hinder implementation. Bilateral initiatives in technology transfer, AI training, and joint R&D could strengthen Indonesia's cyber resilience.

Table 1. Comparative Analysis of Cybersecurity Governance: Indonesia vs. Japan (Author's analysis, 2025)

Dimension	Indonesia	Japan
Governance	Fragmented across BSSN, Komdigi, BIN, TNI, and Polri; overlapping mandates create redundancy. Draft Cybersecurity and Resilience Bill (RUU KKS) seeks centralization but remains pending [15,24,9,4].	Centralized under NISC within the Cabinet Secretariat; ensures cross-ministerial coordination, engages private sector, and integrates cyberterrorism into national security planning [25,15,26].
Legal Frameworks	UU ITE (2008, amended 2016 & 2024) and Anti-Terrorism Law (UU No. 5/2018) address cybercrime and terrorism separately, creating legal ambiguity. Lack of Budapest Convention ratification limits global alignment [22,23,24,8,20].	Cybersecurity Basic Act (2014, revised 2021) provides a unified framework linking digital and national security. Supplemented by Unauthorized Computer Access Law (1999) and APPI. Harmonized with international law via Budapest Convention [25,20,15].
PPPs	Ad hoc and reactive. BSSN collaborates with ISPs, banks, and APJII primarily during major incidents; limited SME investment and low digital literacy constrain effectiveness [11,9,4].	Institutionalized PPPs through J-CSIP and ISACs. Regular cyber drills, structured incident reporting, and NICT-led R&D programs strengthen resilience [26,15].
Intelligence Sharing	Siloed across BIN, BSSN, TNI, and Polri, with limited trust and weak cross-agency exchange. RUU KKS proposes establishment of a National Cyber Operations Centre (NCOC) and	Integrated under NISC, which coordinates intelligence across ministries and with critical infrastructure operators. Japan also engages internationally (ASEAN, G7, U.S., EU),

Dimension	Indonesia	Japan
	Early Warning System (EWS), but implementation remains uncertain [15,9,4].	leveraging AI-based threat detection [26,25,15].
Technological Innovation	Lagging behind regional peers. AI-based anomaly detection pilots exist under BSSN, but implementation is hampered by shortages of skilled personnel and reliance on foreign vendors [9,15,4].	Advanced innovation ecosystem: leadership in AI, 5G, quantum computing, blockchain, and post-quantum cryptography. Emerging technologies embedded into national cybersecurity strategy [26,25,15].

Summary

Japan's centralized, norm-driven, and innovation-oriented model provides valuable lessons for Indonesia, particularly in governance integration, PPP structuring, and legal coherence. However, Japan's reliance on advanced technologies and international regimes also introduces external dependencies [26,25]. Indonesia's sovereignty-centred approach may allow greater national control, but at the cost of slower institutional consolidation. A legislator from DPR RI noted: "Indonesia must learn from Japan, but adapt the model to our own political culture and sovereignty needs" [Author's Interview, Jakarta, 2024].

5 AI, Digital Economy, and Strategic Infrastructure

5.1 Rise of Indonesia's Digital Economy

Indonesia is undergoing one of the most rapid digital transformations in Southeast Asia. The e-Conomy SEA Report projects that Indonesia's digital economy will exceed USD 130 billion by 2025, positioning it as the largest in the region [14]. This growth is driven by a young and tech-savvy population, rising smartphone penetration, and the expansion of e-commerce, fintech, and digital services. According to the Indonesian Internet Service Providers Association [15], internet penetration has surpassed 80%, laying a strong foundation for digital-based growth.

As one analyst observes, "Indonesia's digital economy is no longer peripheral; it is central to the nation's economic strategy and its aspiration to become a digital hub in Asia" [15]. Yet, this rapid growth also creates new vulnerabilities. Critical sectors such as healthcare, finance, and logistics are becoming increasingly digitized and interdependent, creating attractive targets for both state and non-state actors engaged in hybrid warfare [15].

5.2 Institutional Transformation

Recognizing these challenges, Jakarta has initiated a significant institutional shift: the restructuring of the Ministry of Communication and Informatics (Kominfo) into the Ministry of Digital Affairs (Komdigi). This reform reflects a strategic emphasis on digital sovereignty and cybersecurity resilience. Komdigi's mandate is to centralize oversight of data governance, cybersecurity, and AI regulation, while coordinating with the National Cyber and Crypto Agency (BSSN) and the National Counterterrorism Agency (BNPT) [17,18].

Scholars argue that such reforms are critical since "fragmented governance creates gaps that hybrid threats and cyberterrorists can exploit" [2]. Lindsey [16] further notes that fragmented regulatory authority has historically undermined Indonesia's ability to enforce effective cybersecurity policy, making Komdigi's establishment a timely move toward policy coherence.

5.3 Japanese Investment in Strategic Infrastructure

Japan has become a key strategic partner in Indonesia's digital modernization. Firms such as NTT, SoftBank, and Mitsubishi have invested heavily in data centres, submarine cables, smart city projects, and 5G infrastructure [2]. These facilities are critical not only for economic growth but also for national security, given their role in hosting sensitive governmental, financial, and identity data.

A policy report cautions that "foreign investment in digital infrastructure enhances connectivity but also raises dependency risks if not safeguarded by robust cybersecurity frameworks" [14]. Kristiadi [15] similarly warns that while foreign investment can drive technological transfer, it may also create strategic leverage and dependency concerns. Accordingly, the Indonesia–Japan partnership is evolving beyond conventional infrastructure cooperation into a strategic digital alliance, where cybersecurity guarantees form an integral part.

5.4 AI Risks and Opportunities

The integration of artificial intelligence (AI) into Indonesia's digital ecosystem presents a dual-edged challenge. On the risk side, AI is increasingly weaponized for disinformation and psychological operations. AI-generated deepfakes, automated bot networks, and micro-targeted propaganda campaigns threaten electoral integrity and societal cohesion [11].

As Balzacq [12] argues in securitization theory, "technologies of communication become technologies of insecurity when framed as existential threats." Dunn Cavelty [4] similarly highlights that disinformation is now a core instrument of hybrid warfare.

On the opportunity side, AI offers transformative potential for predictive cybersecurity, anomaly detection, and early-warning systems. Machine learning can detect irregular patterns in real time, enabling rapid responses to attacks on critical infrastructures such

as finance, energy, transport, and health [13]. Beyond security, Indonesia is also deploying AI for smart governance, including disaster management and digital public service delivery. This dual role reflects what Dunn Cavelty [4] describes as the "securitization paradox of digital innovation"—where technology represents both the problem and the solution.

5.5 Policy Implications: Public–Private Partnerships and Regional Cooperation

The convergence of AI, digital economy, and strategic infrastructure highlights the need for robust, multi-layered policy responses:

Public–Private Partnerships (PPPs): Collaborative frameworks involving Komdigi, BSSN, Telkom Indonesia, Gojek-Tokopedia (GoTo), and international partners such as Microsoft, Google Cloud, and Japanese investors are central to Indonesia's cybersecurity posture [7]. Hoffman [8] emphasizes that PPPs are critical for trust-building in addressing asymmetric cyber threats.

Regional Cooperation: Indonesia participates in ASEAN frameworks such as the ASEAN Cybersecurity Cooperation Strategy 2021–2025 and the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok [14]. Japan contributes through investment, policy dialogue, capacity building, and technical transfer [11]. Buzan and Wæver [2] note that such cooperation reflects regional security complex dynamics, linking states' threat perceptions and security practices.

AI Governance: Policymakers must balance economic growth with concerns over algorithmic bias, disinformation, and malicious exploitation [16]. A co-regulatory model, where industry develops standards under government oversight, is suggested.

Digital Sovereignty vs. Global Interoperability: Indonesia's focus on local data governance must be reconciled with participation in transnational cybersecurity frameworks [15].

6 Joint Initiatives and Regional Implications

6.1 Bilateral Frameworks and Strategic Partnership

Since 2019, Indonesia and Japan have gradually institutionalized cybersecurity cooperation through bilateral Memoranda of Understanding (MoUs), high-level dialogues, and their joint participation in multilateral platforms such as the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok [14]. ASEAN [14] has described the AJCCBC as "a central hub to train ASEAN officials and promote interoperability in cybersecurity practices."

The adoption of the ASEAN–Japan Comprehensive Strategic Partnership (CSP) in 2023, during the 50th Anniversary of ASEAN–Japan Friendship and Cooperation,

marked a decisive step in aligning cybersecurity with broader strategic cooperation [14]. The CSP's Joint Vision Statement underscores digital transformation, economic security, and resilience as shared priorities [14]. Its Implementation Plan explicitly highlights cybersecurity collaboration as a strategic workstream, framing it within a trust-based regional security architecture [14].

At the 27th ASEAN–Japan Summit in Vientiane (October 2024), leaders reaffirmed this commitment, emphasizing digital transformation (DX), critical infrastructure protection, and the central role of AJCCBC as a hub for training and coordination [11,14]. As Buzan and Wæver [2] remind us, such institutionalized cooperation is not merely technical: it embeds states in "regional security complexes, where interdependence shapes threat perceptions and responses."

6.2 Operational Cooperation in Cybersecurity

Operational collaboration has also progressed from policy dialogue to practical exercises. At the 16th ASEAN–Japan Cybersecurity Policy Meeting in Tokyo (October 2023), cooperation was reviewed across nine domains, including mutual notification, incident response, cyber drills, critical information infrastructure protection (CIIP), awareness raising, and government–industry–academia linkages [14].

One notable outcome was the drafting of the ASEAN–Japan Cybersecurity Reference Handbook, which, for the first time, introduced structured public–private partnership (PPP) frameworks into the ASEAN context [14]. The 17th Policy Meeting in Singapore (October 2024) consolidated this progress by launching additional joint cyber drills and tabletop exercises.

A CIIP workshop held in Hanoi in August 2023, for example, provided a venue for ASEAN Member States (AMS) and Japan to exchange lessons on R&D investment, maturity assessment, and resilience testing [14]. These exercises operationalize what Valeriano and Maness [10] describe as the "day-to-day management of cyber conflict, where resilience is as important as deterrence."

6.3 PPP Ecosystem Building

Indonesia's draft Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) introduces a framework for mandating PPPs in the cybersecurity domain. Its provisions outline mandatory incident reporting, vendor security certification, and collaborative threat intelligence exchange [15].

Japan's long-standing Cybersecurity Council model demonstrates the institutional value of PPPs by embedding industry and academia into national security governance [14]. Hoffman [8] stresses that "without robust PPPs, counter-terrorism in cyberspace cannot address the asymmetric advantage of non-state actors." Indonesia's PPP

ecosystem thus reflects both a legal mandate and a strategic necessity for reducing fragmentation in cyber resilience.

6.4 Legal Harmonization and Alignment

The RUU KKS also represents Indonesia's attempt to harmonize national regulations with ASEAN frameworks such as the ASEAN Cybersecurity Cooperation Strategy 2021–2025 and to align with global norms codified in Japan's Cybersecurity Basic Act [15,14].

Legal harmonization is more than technical: as Balzacq [12] argues, "institutional alignment transforms securitizing speech acts into legitimate governance practices." This ensures that policy rhetoric around "cyberterrorism" and "hybrid threats" is translated into enforceable legal standards. Such convergence strengthens jurisdictional clarity for investigating transnational cybercrime, reduces safe havens for malicious actors, and improves the interoperability of regional security protocols.

6.5 Expanding Communities of Practice: AJCCA

Beyond intergovernmental frameworks, cross-sectoral communities of practice have emerged. The ASEAN–Japan Cybersecurity Community Alliance (AJCCA), founded during the International Conference on ASEAN–Japan Cybersecurity Community in Tokyo (October 2023), brings together nine cybersecurity communities from ASEAN states and Japan [14].

The AJCCA Memorandum of Understanding commits members to threat intelligence sharing, joint training programs, and collaborative awareness campaigns [14]. This expansion reflects a trend toward multi-actor governance in cybersecurity. As Dunn Cavelty [4] notes, "infrastructural power in cyberspace increasingly depends on dispersed networks of trust between states and non-state actors." The AJCCA Conference in Singapore (2024) reaffirmed this principle by focusing on cyber resilience as a regional public good.

6.6 A Replicable Bilateral–Regional Model

Indonesia–Japan cybersecurity cooperation now illustrates a replicable bilateral–regional model grounded in five interlocking pillars:

1. Law & Policy – RUU KKS, ASEAN CSP, Japan's Cybersecurity Basic Act [15,14];
2. Institutions – BSSN–NISC linkages, AJCCBC, AJCCA [14,17];
3. Capabilities – joint cyber drills, CIIP maturity workshops, policy dialogues [10];
4. Technology – cooperative R&D, AI-enabled threat detection, standard-setting [13];

5. Public–Private Partnerships – mandated collaboration between state and private operators [8,15].

This model embodies what Korybko [9] terms hybrid warfare adaptation: "the convergence of conventional and unconventional domains into an integrated resilience framework." Scaled across ASEAN, such a model offers a cohesive and interoperable response architecture that surpasses fragmented national strategies.

7 Findings and Discussion

7.1 Securitization and Legal Reform

The drafting of the RUU KKS illustrates Indonesia's pivot toward securitization in cyberspace. By framing cybersecurity not merely as a technical or economic concern but as an existential matter of national security, Indonesian policymakers deploy a securitization logic akin to Buzan, Wæver, and de Wilde [2], where "security issues are constructed through speech acts that enable extraordinary measures." This framing legitimizes extraordinary interventions, allowing the state to justify institutional reforms, expand the mandates of agencies such as BSSN, and integrate cyberterrorism into a broader counterterrorism architecture.

As Lindsey [16] argues, "Indonesian security policy has historically been reactive, with legal reforms often following crisis events." In this respect, the RUU KKS represents a significant departure: a proactive attempt to consolidate and bridge gaps left by the UU ITE [22,23] and the UU Terorisme [24]. By codifying cybersecurity as a core domain of national defence, Indonesia institutionalizes cyberspace governance as a securitized field, capable of triggering extraordinary protective measures.

7.2 Hybrid Warfare and Cyberterrorism

A key finding is that cyberterrorism cannot be isolated from the broader spectrum of hybrid warfare. Korybko [9] emphasizes that hybrid warfare "integrates conventional and unconventional methods—military, economic, informational, and cyber—in order to exploit asymmetries." In Indonesia and Southeast Asia more broadly, cyberterrorist groups and their sympathizers blur boundaries between disinformation campaigns, online recruitment, and the potential sabotage of critical infrastructures.

Hoffman [8] notes that "terrorism in the digital era adapts to exploit the vulnerabilities of open, networked societies." This adaptability underscores Indonesia's structural vulnerabilities—not only in the protection of critical infrastructure, but also in its fragmented governance, where overlapping mandates between BSSN, Kominfo/Komdigi, and law enforcement dilute response coherence. Cyberterrorism here is not an isolated digital threat, but one embedded in hybrid campaigns that leverage social, economic, and political dimensions to destabilize states.

7.3 AI as Dual-Use

AI is emerging as a dual-use technology in Indonesia's cybersecurity ecosystem. On the defensive side, AI enables anomaly detection, predictive analytics, and early-warning systems, enhancing resilience against sophisticated threats. However, the same technologies lower barriers for malicious actors. AI-driven deepfakes, automated phishing, and bot-driven disinformation campaigns pose significant risks to electoral integrity and societal trust [11,4,18].

Brundage et al. [7] highlight the dilemma succinctly: "the dual-use nature of AI technologies creates a security dilemma: tools designed for beneficial purposes can be easily weaponized." Similarly, Dunn Cavelty [4] observes that "technological acceleration often outpaces regulatory capacity, creating policy vacuums that adversaries exploit." Indonesia's RUU KKS introduces hooks for AI regulation and governance, but its provisions remain nascent. The lack of integration with broader ethical and digital resilience frameworks means that the country is still vulnerable to AI-enabled hybrid threats.

7.4 PPPs as Strategic Multipliers

PPPs have emerged as strategic multipliers in Indonesia's cybersecurity architecture. Given that most of Indonesia's digital infrastructure is privately owned or operated by multinational companies, state capacity remains constrained without institutionalized cooperation. The RUU KKS formalizes PPPs by introducing mandatory information-sharing obligations, incident reporting, and joint cyber exercises [15,8].

As Dunn Cavelty and Suter [4] argue, "cybersecurity governance cannot be monopolized by the state; it requires a networked approach that integrates both public and private actors." This resonates strongly in Indonesia, where interviewees from BSSN and CSIRT.ID [17] stressed that "without PPP frameworks, Indonesia will remain reactive, dependent on ad hoc cooperation." In this sense, PPPs serve as force multipliers for resilience, positioning Indonesia closer to Japan's well-established PPP councils and ASEAN's collaborative structures.

7.5 Regional Implications

The RUU KKS also holds regional implications, particularly by aligning Indonesia's domestic reforms with ASEAN's *Cybersecurity Cooperation Strategy 2021–2025* [14] and Japan's *Cybersecurity Basic Act* [14]. This alignment demonstrates Indonesia's intent to not only safeguard its national cyberspace but also contribute to regional collective resilience. The AJCCBC in Bangkok, for example, provides a platform where Indonesia can translate domestic securitization into shared norms and training regimes [14]. The comparative positioning of Indonesia, Japan, and ASEAN in key cybersecurity dimensions is summarized in **Table 2**, which highlights the structural linkages between national strategies and regional cooperation frameworks.

Balzacq [12] reminds us that securitization is "embedded in international social fields where alliances, norms, and shared frameworks shape the security agenda." In this context, Indonesia's domestic legal consolidation cannot be disentangled from its regional obligations. The Indonesia–Japan track illustrates how bilateral cooperation can scale into regional blueprints, diffusing best practices across ASEAN through a five-pillar architecture: law and policy, institutions, capabilities, technology, and PPPs [14,15,8].

Table 2. Comparative Findings: Indonesia, Japan, and ASEAN
(Author's analysis, 2025)

Theme	**Indonesia – Key Evidence**	**Japan – Key Evidence**	**ASEAN/Regional – Key Evidence**
7.1 Securitization & Legal Reform	RUU KKS frames cyber as national security, moving beyond UU ITE/UU Terorisme; proactive consolidation consistent with securitization logic. Interviewees stress mandate expansion for BSSN [2,16].	Cybersecurity Basic Act operationalizes securitization across ministries; legal clarity enables coordinated risk governance [2].	ASEAN strategies normalize cyber as regional security; AJCCBC institutionalizes training that embeds securitization [14].
7.2 Hybrid Warfare & Cyberterrorism	Hybrid threats observed (disinformation + probing of CIIs); governance fragmentation increases exposure [9,8].	Integrated doctrine links cyber with info-ops and economic security; past incidents shaped whole-of-government posture [8].	ASEAN acknowledges cross-border hybrid vectors; handbooks/exercises treat cyberterrorism as part of hybrid campaigns [14].
7.3 AI as Dual-Use	Stakeholders see AI as both risk amplifier (deepfakes, phishing) and defence enabler (detection, early warning) [7,4,18].	Strategic use of AI for predictive defence and CIIP monitoring; strong R&D–policy pipeline [4].	Regional training now includes AI-related issues (threat intel, response), exposing dual-use governance gaps [14,7].
7.4 PPPs as Strategic Multipliers	RUU KKS institutionalizes PPPs (reporting, drills). Interviews: "without PPP frameworks, response stays reactive" [4,12,15].	PPP councils and ISAC-like forums integrate industry into planning and exercises [4].	ASEAN encourages gov–industry–academia collaboration; AJCCBC and policy meetings formalize PPP guidance [14].

Theme	Indonesia – Key Evidence	Japan – Key Evidence	ASEAN/Regional – Key Evidence
7.5 Regional Implications	RUU KKS designed to align with ASEAN norms, enabling cross-border cooperation [14,2].	Japan promotes rules and capacity building, linking bilateral with regional architectures [2,14].	CSP/AJCCBC provide scalable scaffolding to translate bilateral cooperation into ASEAN-wide norms [14].

Synthesis and Policy Takeaways

- Convergence through securitization: Indonesia's RUU KKS moves toward Japan's law-anchored model; ASEAN institutions (e.g., AJCCBC) socialize securitization regionally [2,14].
- Hybrid threat posture: Framing cyberterrorism within hybrid warfare sharpens priorities (CIIP, disinformation) and underscores interagency unity [9,8].
- AI governance balance: Both Indonesia and Japan face AI's dual-use risks; policy must mitigate offensive exploitation while accelerating defensive ML applications [7,4].
- PPPs as force multipliers: Mandates (RUU KKS) combined with institutional venues (Japan's PPP councils; ASEAN industry–government tracks) make PPPs doctrinal rather than ad hoc [4,12,15,14].
- Bilateral-to-regional scaling: The Indonesia–Japan model offers a replicable five-pillar blueprint for ASEAN, enhancing resilience through alignment of law, institutions, capabilities, technology, and PPPs [14,15,8].

8 Conclusion and Policy Recommendations

8.1 Conclusion

The draft Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) represents a pivotal moment in Indonesia's securitization of cyberspace and the institutionalization of cyber governance. By reframing cyber threats as existential challenges to state sovereignty, the bill reflects the logic of securitization outlined by Buzan, Wæver, and de Wilde [2], whereby issues are presented as existential threats that justify extraordinary protective measures.

Indonesia's trajectory mirrors broader regional shifts, as cybersecurity is increasingly framed not as a purely technical matter but as a core element of national defence, hybrid warfare, and resilience-building [9,8]. Bilateral initiatives with Japan—particularly around capacity-building, AI integration, and joint drills—demonstrate how structured cooperation can serve as a replicable model for ASEAN [14]. This is especially urgent in an era where cyberterrorism leverages artificial intelligence, disinformation, and

hybrid influence operations to blur distinctions between state and non-state actors [7,4,18].

In this sense, the RUU KKS is not only a domestic reform but part of ASEAN's broader securitization pivot, embedding law, governance, and technology within a multi-layered regional security architecture [12,14,15].

8.2 Policy Recommendations

For Indonesia:

1. Enact RUU KKS with clarity of scope and mandates. Legal ambiguities—particularly between the UU ITE [22,23] and the UU Terorisme [24]—must be resolved to avoid jurisdictional overlap or enforcement vacuums [2,16].
2. Strengthen institutional coordination between BSSN and Komdigi. Governance fragmentation reduces agility; cybersecurity must be treated as a political process rather than only a technical fix [4].
3. Invest in AI-driven defensive capacities. Beyond detection, AI should function as a resilience multiplier against disinformation and hybrid influence campaigns [7].

For Japan:

1. Support Indonesia's legal transition. Japan's Cybersecurity Basic Act (2014, revised 2021) provides a benchmark for embedding resilience in national security frameworks [14].
2. Co-develop AI-enabled defence tools. Joint research and development initiatives under METI–BSSN cooperation would accelerate preparedness across the region [13].
3. Share best practices in PPPs. Japan's structured approach to public–private partnerships—anchored in its Cybersecurity Strategic Headquarters—offers a model for Indonesia's nascent PPP framework institutionalized in the RUU KKS [19,20].

For ASEAN:

1. Harmonize legal frameworks. Cross-border cyberterrorism requires interoperable legislation, aligned with the ASEAN Cybersecurity Cooperation Strategy 2021–2025 [14].
2. Institutionalize the ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC). Moving beyond project-based cooperation toward a permanent institutional framework would ensure long-term capacity building [11,14].
3. Strengthen collective digital sovereignty. ASEAN must balance external dependencies with indigenous capacity, reflecting the view of "cyber sovereignty as an extension of national sovereignty in the digital domain" [15].

8.3 Final Reflection

Cyberterrorism in the AI era is not a singular or isolated threat but a convergence of asymmetric warfare, technological disruption, and governance fragmentation. Responses must move beyond piecemeal technical measures and instead integrate law, governance, and technology into a holistic security architecture [8,9,7,4].

As Hoffman [8] reminds us, terrorism evolves alongside technological advances, and cyberspace is now the battlespace of asymmetric actors. By institutionalizing cyber governance through the RUU KKS, strengthening bilateral cooperation with Japan, embedding frameworks such as AJCCBC at the regional level, and deploying AI responsibly, Indonesia and ASEAN can set a precedent for Southeast Asia in countering the evolving hybrid spectrum of cyberterrorism [14,15,8].

Acknowledgments. The authors would like to express sincere gratitude to the **School of Strategic and Global Studies, Universitas Indonesia**, for providing academic support throughout this research. Special thanks are also extended to the **Badan Siber dan Sandi Negara (BSSN)**, **Badan Nasional Penanggulangan Terorisme (BNPT)**, and colleagues from the **ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC)** for their invaluable insights and resources that enriched the comparative analysis of this study. Finally, appreciation is given to mentors, peers, and reviewers whose constructive feedback has strengthened the quality and clarity of this manuscript.

Disclosure of Interests. The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article. The research was conducted independently for academic purposes as part of doctoral and faculty research activities at the School of Strategic and Global Studies, Universitas Indonesia.

References

1. Arquilla, J., Ronfeldt, D. (eds.): Networks and netwars: The future of terror, crime, and militancy. RAND Corporation, Santa Monica (2001)
2. Buzan, B., Wæver, O., de Wilde, J.: Security: A new framework for analysis. Lynne Rienner, Boulder (1998)
3. Denning, D.E.: Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In: Arquilla, J., Ronfeldt, D. (eds.) Networks and netwars: The future of terror, crime, and militancy, pp. 239–288. RAND Corporation, Santa Monica (2001)
4. Dunn Cavelty, M.: Cyber-security and threat politics: US efforts to secure the information age. Routledge, London (2008)
5. Fairclough, N.: Critical discourse analysis: The critical study of language. Longman, London (1995)
6. Foucault, M.: Discipline and punish: The birth of the prison. Pantheon, New York (1977)
7. Brundage, M., Avin, S., Clark, J., et al.: The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv:1802.07228 (2018)
8. Hoffman, B.: Inside terrorism, 2nd edn. Columbia University Press, New York (2006)
9. Korybko, A.: Hybrid wars: The indirect adaptive approach to regime change. Peoples' Friendship University of Russia, Moscow (2015)

10. Valeriano, B., Maness, R.: Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press, New York (2015)
11. Mumford, A.: Proxy warfare. Polity, Cambridge (2013)
12. Balzacq, T.: A theory of securitization: Origins, core assumptions, and variants. In: Balzacq, T. (ed.) Securitization theory: How security problems emerge and dissolve, pp. 1–30. Routledge, London (2011)
13. Jarvis, L., Macdonald, S.: Cyberterrorism: Understanding, assessment, and response. Springer, Cham (2015)
14. OECD: OECD digital economy outlook 2020. OECD Publishing, Paris (2021). https://doi.org/10.1787/bb167041-en
15. Kristiadi, J.: Cybersecurity governance in Indonesia: Between national security and digital economy. Journal of ASEAN Studies 5(1), 45–62 (2017)
16. Lindsey, T.: Indonesian law and society in the digital era. In: Lindsey, T., Butt, S. (eds.) Indonesian law and society, pp. 301–322. Federation Press, Sydney (2018)
17. Badan Siber dan Sandi Negara (BSSN): Annual report of BSSN 2020. BSSN, Jakarta (2021)
18. Dunn Cavelty, M.: The social dimensions of security: Technological threats, risk perception, and governance. Routledge, London (2014)
19. Renz, B.: Russia and hybrid warfare. Routledge, London (2016)
20. Jarvis, L., Renz, B.: Cybersecurity policy lessons: Japan's PPP experience. International Affairs 98(3), 1–20 (2022)
21. Badan Nasional Penanggulangan Terorisme (BNPT): Counter-terrorism strategy 2020–2024. BNPT, Jakarta (2020)
22. Republic of Indonesia: Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) (2008)
23. Republic of Indonesia: Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions (2016)
24. Republic of Indonesia: Law No. 5 of 2018 amending Law No. 15 of 2003 on the Eradication of Terrorism Crimes (2018)
25. Dewan Perwakilan Rakyat Republik Indonesia (DPR RI): Academic manuscript of the Draft Law on Cybersecurity and Cyber Resilience (RUU KKS). DPR RI, Jakarta (2023)
26. Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo): Indonesia digital roadmap 2021–2024. Kominfo, Jakarta (2022)
27. Kementerian Pertahanan Republik Indonesia: Indonesian defense white paper. Ministry of Defense, Jakarta (2020)
28. ASEAN: ASEAN Cybersecurity Cooperation Strategy 2021–2025. ASEAN Secretariat, Jakarta (2021)
29. NATO: NATO 2030: United for a new era. NATO Public Diplomacy Division, Brussels (2020)
30. United Nations Office of Counter-Terrorism (UNOCT): Countering terrorist use of new and emerging technologies. United Nations, New York (2021)
31. World Economic Forum (WEF): Global risks report 2022. World Economic Forum, Geneva (2022)
32. Mumford, A.: Hybrid threats and regional stability. Global Policy 10(4), 12–25 (2019)
33. OECD: Digital security governance in Asia-Pacific: Lessons for Indonesia. OECD Publishing, Paris (2022)
34. Hoffmann, F.: Public-private partnerships in cybersecurity: A comparative study. Journal of Cyber Policy 2(3), 45–63 (2017)
35. Brundage, M., et al.: Governance frameworks for AI in national security. Security Dialogue 49(2), 145–165 (2018)

36. Kristiadi, J.: Cyber sovereignty in ASEAN: Legal and institutional perspectives. Asian Journal of International Law 10(2), 210–230 (2020)
37. Dunn Cavelty, M., Suter, M.: Public-private partnerships in cybersecurity: An integrative approach. International Studies Review 11(2), 137–152 (2009)
38. Lindsey, T.: Cybersecurity policy in Indonesia: Lessons from UU ITE. Journal of Southeast Asian Studies 54(2), 200–220 (2023)
39. Jarvis, L., Renz, B.: AI-enabled defense cooperation in ASEAN. Defence Studies 22(1), 55–72 (2022)
40. Kominfo & BSSN: Cyber drills and capacity-building report 2023. Jakarta (2023)
41. ASEAN: ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC) report 2023. ASEAN Secretariat, Bangkok (2023)
42. BSSN & CSIRT.ID: Expert interviews 2024, Jakarta (2024)
43. Valeriano, B., Maness, R.: Day-to-day management of cyber conflict: Cyber exercises and resilience. International Journal of Cyber Warfare 7(1), 34–51 (2015)