LAB 45 — TELAAH KEBIJAKAN

No. 002 - 18 Maret 2025

Telaah Kebijakan LAB 45 adalah wadah yang dirancang untuk menyampaikan pandangan kritis dan analisis terkini dari para peneliti serta analis kebijakan terkait berbagai isu strategis seputar politik keamanan, ekonomi politik, politik media, dan gender. Platform ini bertujuan untuk memberikan wawasan mendalam sekaligus menawarkan gagasan inovatif dalam menghadapi tantangan lokal ataupun global. Pendapat yang tercantum dalam setiap komentar merupakan tanggung jawab penulis sepenuhnya dan tidak merefleksikan posisi resmi LAB 45. Jika Anda memiliki pertanyaan atau memerlukan informasi lebih lanjut, silakan menghubungi tim kami melalui lab45@lab45.id.

Indonesia's Cyber Security and Resilience Bill: Strengthening Governance or Expanding Institutional Rivalries?

Christian Guntur Lebang
Analis Utama Politik Keamanan, Laboratorium Indonesia 2045

As Indonesia moves forward with the Cyber Security and Resilience Bill (RUU KKS) in 2025, a leaked draft has sparked debates over its potential impact on cyber governance. The bill aims to strengthen the National Cyber and Crypto Agency (BSSN), but its provisions on content filtering, AI regulation, and law enforcement powers raise concerns about overlapping roles with other key institutions, such as the Ministry of Digital and Communications (Kemkomdigi) and the National Police (Polri). With multiple agencies vying to maintain or expand their authority in cyberspace, the bill could either streamline cybersecurity governance or deepen existing institutional rivalries, shaping the future of Indonesia's digital security framework.

Background and Legislative Developments

Since the establishment of BSSN in 2017, the Indonesian government has sought to enact a comprehensive cybersecurity law. However, previous attempts failed due to political sensitivities and concerns over potential infringements on privacy. To address the regulatory gap, the government issued three presidential regulations to provide interim cybersecurity governance. The first regulation established BSSN's structure and outlined its core responsibilities. The second focused on the protection of vital information infrastructure, ensuring key sectors have cybersecurity safeguards in place. The third regulation, which was originally drafted as two separate policies but later merged to streamline the process, covers the national cybersecurity strategy and cyber crisis management. While these regulations provide a temporary framework, they lack the legal weight of a dedicated cybersecurity law, prompting the renewed push for RUU KKS.

In November 2024, the government and parliament included RUU KKS among 41 legislative priorities for 2025. Unlike the 2019 attempt, which was initiated by parliament, this version is government-sponsored, with renewed urgency following a major ransomware attack on Indonesia's national data centre. The attack, attributed to the Brain Cipher ransomware group, disrupted over 200 government institutions, including critical services such as immigration and education, drawing public attention to the country's cybersecurity

vulnerabilities.

With a new administration under President Prabowo Subianto, leadership changes at BSSN was initially would influence the bill's trajectory. In December 2024, the Indonesian Military Commander, General Agus Subiyanto, issued a tour-of-duty decree appointing Lieutenant General Nugroho Sulistyo Budi, a long-time intelligence official, as the new head of BSSN. This raised questions about whether the drafting process would be delayed to accommodate his input. However, a draft of the bill was unexpectedly circulated in late February 2025, catching stakeholders off guard. The draft is currently being deliberated within an inter-ministerial committee (PAK), where various agencies are providing input before it moves to parliament for further discussion.

Institutional Overlaps and Competing Authorities

The bill is expected to provoke tensions among government agencies, particularly BSSN, Kemkomdigi, and Polri, all of which have overlapping interests in cyber governance. Since BSSN's inception, efforts to delineate institutional responsibilities have been met with resistance. The proposed legislation was initially expected to resolve these ambiguities by clearly defining roles. However, the current draft appears to expand BSSN's mandate without sufficiently clarifying its relationship with existing agencies.

One contentious provision is Article 69, which grants BSSN the authority to filter content deemed a cyber threat. This role traditionally falls under Kemkomdigi, which enforces the Electronic Information and Transactions Law (UU ITE) and oversees content removal related to pornography, online gambling, and public order disruptions. The broad language of Article 69 raises concerns over potential jurisdictional conflicts, particularly as BSSN's past leadership has described harmful online content as a form of "social cyber-attack," creating ambiguity in its implementation. If passed, this provision would set a regional precedent, as no other democratic country's cybersecurity agency holds such authority. For comparison, Australia, Singapore, and Malaysia exclude content filtering from their cybersecurity laws, delegating such responsibilities to other regulatory bodies. Civilian cybersecurity agencies in these countries also oversee foreign misinformation campaigns, particularly during elections. However, their focus is on public awareness campaigns and information sharing with law enforcement rather than direct content filtering. In contrast, China's Cyberspace Administration exercises sweeping control over online content, a model unlikely to align with Indonesia's democratic framework.

Another area of concern is the bill's provisions on artificial intelligence (AI). The draft introduces the concept of "products with digital elements" (PDED), as outlined in Articles 10-14, inspired by the European Union's Cyber Resilience Act (CRA), which includes smart devices and software. This broad definition raises questions about whether generative AI platforms and other software applications will fall under BSSN's regulatory scope. Additionally, Article 43 grants BSSN the authority to regulate the use of AI in protecting critical information infrastructure (CII) from cyber threats. While the coordination of CII protection already falls under BSSN's mandate, regulating how AI should be used in this context is a new development for the agency. This provision raises concerns about its overlap with Kemkomdigi, which has traditionally led AI governance efforts, including issuing an AI ethics circular in 2023. If passed, it could position BSSN as the primary authority on AI-driven cybersecurity, intensifying institutional competition. Given the absence of a dedicated AI regulatory body in Indonesia, the bill's passage in its current form is likely to face resistance from Kemkomdigi and calls for a distinct AI governance framework.

The most controversial provision, however, is Article 82, which grants BSSN investigative authority over cyber-related crimes. If enacted, BSSN would become a law enforcement entity, a significant departure from standard practices where cybersecurity agencies primarily focus on threat intelligence and coordination. Traditionally, criminal

investigations fall under the jurisdiction of Polri and the Attorney General's Office (Kejagung). While the current draft states that the arrest process must still adhere to the Criminal Procedure Code—limiting arrest authority to Polri and Kejagung—it leaves room for BSSN to seize assets deemed important for investigations, raising concerns about the extent of its enforcement powers. Allowing BSSN to conduct investigations may deter cyber incident reporting, as victims could fear criminal sanctions. Unlike Australia's Cyber Security Act, which protects reported information from being used as legal evidence, the Indonesian bill lacks similar safeguards, raising concerns about legal risks for businesses and individuals reporting cyber incidents.

Response from Other Institutions

Beyond BSSN, other agencies are manoeuvring to expand their influence in cyber governance. Following its restructuring in October 2024, Kemkomdigi introduced new directorates, including the Directorate for Artificial Intelligence and New Tech Ecosystem and the Directorate for Digital Investigation—both of which directly overlap with BSSN's proposed new roles. Minister Meutya Hafidz has also signalled plans to lead a new government regulation aimed at integrating financial systems into the fight against illegal online gambling, which could intersect with BSSN's regulatory scope.

Meanwhile, Polri is seeking greater authority in cyberspace, particularly through the proposed revision of the National Police Law. Last year's draft indicated that Polri wants the power to block and restrict online access, a move that some observers view as a response to a 2019 court ruling that deemed internet blackouts during Papua protests unlawful. Additionally, Polri sought wiretapping authority—an action generally understood to require a distinct regulation—raising further concerns about the scope of its cybersecurity role. If successful, this revision could further complicate the cybersecurity regulatory landscape.

The Indonesian military (TNI) is also likely to push for a greater role in cybersecurity. President Prabowo's policy of appointing military officials to civilian positions suggests that TNI may seek deeper involvement in broader governance. This has fuelled criticism from experts who argue that Prabowo is rolling back military reforms and steering the country back toward the New Order era. Separately, TNI has long perceived online criticism as part of information warfare and has sought a law enforcement role specifically to counter such threats. Although plans to establish a dedicated cyber force appear to have stalled, TNI's persistent interest in cyber operations suggests it will remain a key stakeholder in future policy discussions.

Conclusion

The ongoing deliberation of the RUU KKS underscores the complexities of Indonesia's cyber governance landscape. While the bill aims to enhance national cybersecurity, its broad provisions risk exacerbating inter-agency competition and creating legal uncertainties. The expansion of BSSN's authority—particularly in content filtering, AI regulation, and law enforcement—raises concerns over jurisdictional conflicts with Kemkomdigi, Polri, and even TNI. Another key factor is BSSN's new leadership, which has close ties to President Prabowo, having served in both a special military unit under his command and later at the Ministry of Defence during his tenure. This connection suggests that the President may fully support the bill, strengthening BSSN's position and making it more difficult for other agencies to push back against its expanded authority. Additionally, civil society organizations and private companies may view the bill as overly expansive, fearing regulatory overreach and increased government control over digital spaces. Without clearer delineation of institutional responsibilities and safeguards against misuse, the legislation could introduce more governance challenges than solutions, potentially reshaping Indonesia's cybersecurity landscape in unintended ways.

Referensi:

Kompas. “RUU Keamanan dan Ketahanan Siber Dibatalkan, Ini Alasannya.” Accessed on 11 March 2015. https://nasional.kompas.com/read/2019/09/27/18241611/ruu-keamanan-dan-ketahanan-siber-dibatalkan-ini-alasannya

Antara. “41 Bills Set for 2025 Legislative Priority List, Key Anti-Corruption Bill Omitted.” Accessed on 10 Maret 2025. https://jakartaglobe.id/news/41-bills-set-for-2025-legislative-priority-list-key-anticorruption-bill-omitted

The Jakarta Post. “More than 40 agencies hit by cyberattack on Kominfo data centers.” Accessed on 11 Maret 2025. https://www.thejakartapost.com/indonesia/2024/06/27/more-than-40-agencies-hit-by-cyberattack-on-kominfo-data-centres.html.

Hukum Online. “Poin-poin Usulan dalam Perancangan RUU Keamanan Siber.” Accessed on 11 Maret 2025. https://jakartaglobe.id/news/41-bills-set-for-2025-legislative-priority-list-key-anticorruption-bill-omitted

Tempo. “Menkomdigi Siap Terbitkan Peraturan Pemerintah untuk Tangani Judi Online.” Accessed on 11 Maret 2025. https://www.tempo.co/politik/menkomdigi-siap-terbitkan-peraturan-pemerintah-untuk-tangani-judi-online-1210133

SAFENet, Analysis of Digital Rights Violation in the National Police Bill. Accessed on 10 Maret 2025. https://safenet.or.id/2024/07/analysis-of-digital-rights-violations-in-the-national-police-bill/

The Jakarta Post. “Proposed TNI Law revision may harm military’s professionalism.” Accessed on 11 Ma 2025. https://www.thejakartapost.com/indonesia/2025/03/06/proposed-tni-law-revision-may-harm-militarys-professionalism.html

The Jakarta Post. “Former Tim Mawar members promoted to Defense Ministry.” Accessed on 10 March 2025. https://www.thejakartapost.com/paper/2020/09/27/former-tim-mawar-members-promoted-to-defense-ministry.html

Jalan Mabes Hankam No. T65, Bambu Apus, Cilangkap, DKI Jakarta 13890
Email: lab45@lab45.id | Telpon: +62811452045

Silahkan hubungi tim editorial untuk pertanyaan melalui lab45@lab45.id