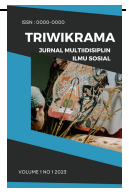
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Vol. 9 No. 4 (2025)
E-ISSN: 2988-1986
Open Access:



KEAMANAN SIBER: RESPON STRATEGIS INDONESIA TERHADAP ANCAMAN DIGITAL

Balqis F. Bintang Semesta

[123] Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

ARTICLE INFO

Article history:
Received Juni, 2025
Revised Juni, 2025
Accepted Juni, 2025
Available online Juni , 2025

balqisfuadybsk@gmail.com

This is an open access article under the CC BY-SA license.
Copyright © 2023 by Author. Published by Universitas Pendidikan Ganesha.

A B S T R A K

Dalam era digital yang semakin kompleks, keamanan siber telah menjadi isu strategis yang menyentuh langsung aspek kedaulatan, pelayanan publik, dan legitimasi pemerintahan. Penelitian ini bertujuan untuk menganalisis bagaimana negara, khususnya Indonesia, merespons ancaman digital yang kian meningkat, terutama setelah insiden besar seperti serangan ransomware terhadap pusat data nasional. Menggunakan pendekatan kualitatif berbasis studi dokumen dan analisis wacana kebijakan, penelitian ini mengeksplorasi kesiapan kelembagaan, regulasi, kapasitas teknis, serta dinamika koordinasi antarinstansi dalam membentuk pertahanan siber nasional. Hasil kajian menunjukkan bahwa meskipun telah ada kemajuan dalam hal pembentukan lembaga seperti BSSN, penyusunan regulasi, serta upaya kerja sama internasional, respons negara masih terfragmentasi dan cenderung reaktif. Kurangnya backup data, minimnya SDM teknis, dan tumpang-tindih kewenangan menjadi hambatan utama. Studi ini menegaskan bahwa penguatan keamanan siber nasional memerlukan sinergi kebijakan yang lebih terpadu, reformasi kelembagaan, dan kepemimpinan yang berorientasi pada pencegahan serta kesiapsiagaan.

Kata Kunci*:* Keamanan siber, Strategi nasional, Respons negara, Ancaman digital, Kebijakan publik.

A B S T R A C T

In today's increasingly complex digital era, cybersecurity has emerged as a strategic issue directly impacting sovereignty, public service delivery, and governmental legitimacy. This study aims to analyze how the Indonesian government responds to escalating digital threats, especially in the wake of major incidents such as the ransomware attack on the national data center. Using a qualitative approach based on document analysis and policy discourse review, this research explores institutional readiness, regulatory frameworks, technical capacity, and inter-agency coordination in shaping national cyber defense. The findings indicate that although progress has been made such as the establishment of the National Cyber and Crypto Agency (BSSN), development of key regulations, and efforts in international cooperation the state's response remains fragmented and largely reactive. A lack of data backups, limited qualified technical personnel, and overlapping institutional authority pose major challenges. The study concludes that strengthening national cybersecurity requires more integrated policy synergy, institutional reform, and leadership focused on prevention and preparedness.

Keywords: *Cybersecurity, National strategy, State response, Digital threats, Public policy.*

*Corresponding author
E-mail addresses: balqisfuadybsk@gmail.com

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8 No 6, 2025
E-ISSN: 2988-1986
Open Access:

1. PENDAHULUAN

Ruang siber telah berkembang menjadi domain strategis yang krusial bagi negara modern, tidak terkecuali Indonesia. Pada 20 Juli 2023, Presiden Joko Widodo menandatangani Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, menandai titik balik bagi kelembagaan dan regulasi nasional di bidang ini. Meskipun demikian, realitas ancaman yang nyata justru semakin memperkuat urgensi penguatan aturan; kasus peretasan ransomware yang melumpuhkan Pusat Data Nasional (PDN) pada Juni 2024, yang menggunakan varian *LockBit* 3.0 dan menuntut tebusan mencapai USD 8 juta, menjadi bukti betapa kerentannya infrastruktur digital negara. Presiden lalu memerintahkan audit menyeluruh terhadap data center pemerintah setelah diketahui hampir seluruh data tak memiliki sistem cadangan, menyoroti masalah tata kelola dan kesiapsiagaan siber yang selama ini terabaikan (Balqis & Marzaman, 2025).

Kasus kebocoran data pun tak kalah memprihatinkan. Dari e-visa di Bali yang sempat memperlihatkan data sensitif pengguna pada gawai orang lain, kebocoran jutaan data kependudukan BPJS dan Dukcapil, hingga publikasi data paspor dalam forum siberm isalnya pada kuartal pertama 2023, semuanya menunjukkan kelemahan pengamanan data publik dan konsekuensinya: hilangnya kepercayaan publik terhadap lembaga pemerintah. Kondisi tersebut mendorong dibentuknya ekosistem regulasi seperti UU PDP 2022 dan turunan Perpres 2023, termasuk regulasi manajemen insiden dan krisis siber di BSSN. Namun, hingga kini, belum hadir Undang-Undang keamanan siber komprehensif, dan berbagai regulasi sektoral tersebar di BSSN, TNI, Polri, BIN, dan Kominfo tanpa payung hukum yang menyatukan poin yang sering dikritik sebagai celah besar dalam respons nasional (Balqis & Marzaman, 2025).

Di tataran kelembagaan, BSSN yang terbentuk dari penyatuan Lemsaneg dan Direktorat Keamanan Siber Kominfo, menjadi aktor utama dalam menjaga keamanan ruang digital. Tahun 2024, BSSN menerbitkan regulasi baru yakni Perpres 1/2024 dan 2/2024 tentang manajemen insiden dan krisis siber, yang menetapkan standar pelaporan dan pembentukan tim respons insiden (CIRT) sebagai fondasi kesiapsiagaan nasional. Selain itu, muncul wacana pembentukan Angkatan Siber TNI sebuah matra ke-4 baru dalam Tentara Nasional Indonesia yang diperintahkan Presiden pada September 2024 untuk mengantisipasi perang siber yang kian kompleks dan agresif. Langkah ini memperlihatkan bagaimana aktivitas militer siber tak lagi hanya domain pertahanan, tetapi juga bagian dari diplomasi dan kebijakan keamanan nasional (Sudarmadi & Runturambi, 2019).

Peningkatan kapasitas SDM menjadi aspek kunci lain dari strategi nasional. Program pelatihan dan sertifikasi keamanan digital dilakukan bersama mitra global seperti Kaspersky dan Microsoft, sekaligus menanamkan literasi digital kepada masyarakat agar masyarakat lebih tangguh menghadapi praktik phishing, social engineering, dan teknik manipulatif lainnya. Di sisi akademik dan industri, data menunjukkan bahwa tenaga profesional keamanan siber masih minim, sementara kebutuhan akan talenta meningkat drastis fenomena yang diperkuat melalui berbagai indeks yang menunjukkan Indonesia memiliki potensi besar jika dukungan pendidikan dan ekosistem pengembangan dioptimalkan (Sudarmadi & Runturambi, 2019).

Di kancah geopolitik, ancaman siber pun tidak sekadar domestik. Laporan dan pengungkapan seperti serangan yang mengatasnamakan kelompok Mustang Panda (Cina) yang berhasil menjebol jaringan BIN dan beberapa kementerian pada 2021, serta infiltrasi terhadap sistem ASEAN melalui server Microsoft Exchange, menunjukkan bagaimana spionase siber telah meluas ke ranah diplomasi dan keamanan kawasan. Indonesia pun ikut terdampak dalam dinamika ini, mendorong kolaborasi intelijen dan teknis dengan negara tetangga serta aliansi strategis seperti kesepakatan pertahanan Australia–Indonesia termasuk komponen keamanan siber dalam Kerjasama Keris-Woomera (Ariel *et al.*, 2025*)*.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

Meskipun regulasi dan komitmen kelembagaan telah meningkat secara signifikan, masih terdapat kesenjangan implementasi mulai dari koordinasi antar instansi, konsistensi dalam penerapan standar keamanan, hingga sanksi dan payung hukum yang detil. Agenda pembahasan dalam RPJMN 2025–2029 dan dorongan pembentukan Undang-Undang Keamanan dan Ketahanan Siber menjadi sinyal bahwa Indonesia tengah memperkuat landasan strategisnya untuk menghadapi kancah digital yang disruptif.

METODE

Metode dalam studi ini mengadopsi pendekatan kualitatif murni, yang bertumpu pada kajian dokumenter dan literatur sebagai bahan empiris utama. Pendekatan ini memungkinkan peneliti mengeksplorasi dimensi teoretis dan praktik keamanan siber secara mendalam, tanpa interaksi langsung lapangan. Sumber data yang digunakan meliputi regulasi seperti Perpres dan UU PDP, laporan resmi BSSN dan instansi terkait, *white papers* dari badan internasional, artikel ilmiah, serta publikasi media kredibel. Pendekatan dokumenter ini bersifat tidak invasif sekaligus kaya konteks historis dan kelembagaan.

Untuk menganalisis materi teks tersebut, penelitian ini menggunakan metode *content analysis* dan *thematic analysis*. *Content analysis* dilakukan dengan membaca dokumen secara sistematis, mengkode berbagai tema kunci seperti kerangka regulasi, struktur kelembagaan, dan manajemen krisis siber, lalu mengindetifikasi pola berulang dalam data. Analisis tematik kemudian mengembangkan kode tersebut menjadi tema utama dan subtema melalui prosedur reflektif dan induktif, sesuai panduan Braun dan Clarke, memetakan makna eksplisit dan implisit tindakan negara dalam menghadapi ancaman digital.

Keandalan dan validitas hasil dijaga melalui strategi triangulasi. Pendekatan ini menggabungkan kajian dari berbagai jenis dokumen (*data triangulation*), penggunaan dua metode analitis (*methodological triangulation*), serta perspektif teori yang relevan (*theoretical triangulation*). Pendekatan teknik triangulasi seperti ini membantu menegaskan konsistensi temuan dan mengurangi bias subjektif.

Untuk menjaga *trustworthiness*, penelitian ini mengadopsi prinsip Lincoln & Guba termasuk *credibility, dependability,* dan *confirmability*. Dokumentasi proses analisis secara transparan dari pemilihan dokumen, tahapan pengkodean, hingga pengembangan tema dilakukan secara berkelanjutan dan dapat diaudit ulang. *Inter-coder reliability* diuji dengan melibatkan rekan sejawat sebagai *co-analyst* yang secara independen meninjau kode dan tema, lalu dibandingkan tingkat kesepakatannya. Langkah ini bukan hanya memberikan angka reliabilitas, tetapi juga memancing refleksi terhadap posisi peneliti dan asumsi teoretis yang mempengaruhi interpretasi.

Keseluruhan proses analisis kemudian diperkuat melalui audit trail, di mana setiap dokumen, kode, memo refleksi, dan iterasi analisis didokumentasikan secara tertib, memungkinkan telaah ulang dan verifikasi pihak eksternal. Pernyataan refleksivitas juga disertakan, mengungkap posisi peneliti, latar belakang, dan asumsi yang mungkin membentuk cara pandang dan penafsiran data.

HASIL DAN PEMBAHASAN

HASIL

Hasil penelitian menunjukkan bahwa Indonesia menghadapi situasi keamanan siber yang kritis. Data BSSN tahun 2023 menunjukkan sebanyak 418 dari 586 aplikasi pemerintahan dikategorikan "*Critical*", dan lebih dari 2.850 celah keamanan ditemukan pada sistem elektronik

*Corresponding author
E-mail addresses: balqisfuadybsk@gmail.com

pemerintah. Tingkat kerentanan ini diperparah oleh kejadian serius seperti serangan ransomware pada Pusat Data Nasional (PDN/PDNS) Juni 2024, di mana 40 TB data menjadi terenkripsi dan hampir 98 % data Tidak memiliki sistem *backup*, menyebabkan layanan publik lumpuh selama beberapa minggu. Di sisi respons kelembagaan, evaluasi BSSN terhadap Satuan Tugas Pelindungan Data menunjukkan pencapaian "Baik" untuk 24 kementerian/lembaga, dengan skor Indeks KAMI sebesar 594 indikator kesiapan informasi berdasarkan SNI ISO/IEC 27001. Pelatihan, simulasi, serta assesment di BUMN sukses meningkatkan kesiapsiagaan infrastruktur vital seperti PT Pindad, PT LEN, dan PT Krakatau Steel, menurut laporan OpenGov Asia Agustus 2023 (Simorangkir *et al.*, 2024).

Kendati demikian, kelembagaan BSSN belum mampu menjangkau seluruh spektrum keamanan nasional. Penugasan CSIRT masih baru mencapai tahap awal; misalnya tingkat implementasi di sektor publik masih sekitar 52 % menurut studi akademik, terbentur oleh birokrasi dan kurangnya SDM kompeten. Evaluasi kritis juga muncul dari para pakar, misalnya Gildas Deograt dari Formasi menyebut BSSN cenderung reaktif, bukan proaktif, dan menurutnya hanya bertanggung jawab sekitar 20–30 % terhadap penanganan insiden PDNS Juni 2024 (Alfikri & Ahmad, 2022).

Kolaborasi internasional mencerminkan peningkatan kapasitas teknis dan intelijen. Studi tentang kerja sama ASEAN 2019–2021 mencatat BSSN memfasilitasi koordinasi dan pertukaran informasi penting terkait spionase siber dan propaganda wilayah. Ditambah inisiatif Google-BSSN pada 2024 memperkuat kesiapan melalui program sertifikasi, latihan berbasis AI, dan penguatan *threat intelligence* diharapkan mampu menurunkan kerugian hingga IDR 1.365 triliun pada 2030 (Gani, 2023).

Meskipun terdapat kemajuan dalam regulasi dan kerangka nasional, penelitian menemukan adanya fragmentasi hukum Perpres Keamanan Siber tanpa undang-undang dasar yang konsolidatif mengakibatkan duplikasi tanggung jawab antara BSSN, Kominfo, TNI, Polri, dan BIN. Catatan masyarakat sipil dan diskusi publik termasuk komentar Reddit menyoroti isu sumber daya manusia berkualitas dan anggaran yang besar, namun kelemahan dalam struktur kepemimpinan teknis masih berkontribusi pada kegagalan implementasi, seperti backup data dan respons cepat terhadap insiden.

PEMBAHASAN

Pembahasan ini mengidentifikasi keamanan siber sebagai tantangan multidimensional: teknis, kelembagaan, regulatif, serta kultur organisasi. Insiden ransomware yang melanda ke 44 lembaga pemerintah pada Juni 2024, dengan varian *LockBit* 3.0 yang mengenkripsi lebih dari 40 TB data dan memengaruhi imigrasi dan fasilitas bandara utama, memperlihatkan bahwa struktur digital negara meski ambisius melalui inisiatif seperti One Data Indonesia dan super-app pemerintah belum didukung oleh kesiapan teknis dasar seperti backup dan segmentasi data. Kisah ini bukan hanya kegagalan teknologi, tetapi mencerminkan kelemahan tata kelola dan budaya risiko, di mana 98 % data pemerintah tidak dibackup.

Kedalaman struktur kelembagaan terlihat melalui peran ganda BSSN dan Kominfo dalam merespons insiden. Menurut *Channel News Asia*, saat krisis terjadi, Kominfo dan BSSN saling menunjuk pihak lain sebagai pihak yang bertanggung jawab terhadap kesalahan tersebut, mencerminkan fragmentasi peran dalam manajemen krisis digital nasional. Ini diperparah oleh kritik publik yang menyebut prosedur backup terlalu birokratis dan menuntut permintaan anggaran per-*case*, padahal hal ini harusnya menjadi mandatori untuk semua lembaga publik. Kritik ini berujung pada kepercayaan masyarakat yang menurun dan desakan agar pejabat politik yang tidak mampu teknis mundur.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 8, Number 6 2025
E-ISSN: 2988-1986
Open Access:

Dari sudut kapasitas SDM dan teknikal, meski BSSN telah membentuk puluhan CSIRT nasional dan sektoral seperti peluncuran 17 CSIRT pusat dan target pembentukan 121 tim hingga 2024 implementasi masih berada di kisaran 50–52 %, menunjukkan kekosongan di *front-line* operasi siber. Salah seorang pakar menyebut bahwa CSIRT masih berulang pada proses teknis tanpa rekaman historis dan kesiapan forensik, menjadikan mereka reaktif, bukan proaktif. Tantangan ini diperparah dengan sedikitnya tenaga profesional bersertifikasi CISSP atau CSSP kurang dari 150 orang di seluruh negeri. KKemajuan internasional terlihat ketika kolaborasi dengan lembaga global seperti FIRST, APCERT, Google, dan perusahaan keamanan multinasional menciptakan sinergi pengetahuan dan teknis modern. Keikutsertaan Indonesia dalam inisiatif ini berdampak langsung terhadap reputasi global, tercermin dari kenaikan peringkat di ITU *Global Cybersecurity Index* (GCI) dari posisi ke-41 pada 2018 menjadi ke-24 di Asia-Pasifik. Namun, prestasi ini masih jauh dari menjawab kerentanan di tingkat operasional (Sigiro *et al.*, 2023).

Secara regulatif, meski Indonesia telah mengadopsi sejumlah perpres dan undang-undang terkait mulai dari Perpres 18/2020, Perpres 47/2023, Perpres 82/2022, hingga UU PDP 2022 kekosongan payung hukum yang menyatukan respons nasional masih masuk kategori kritis. Archipelago regulasi ini menghadirkan tumpang-tindih kewenangan antara lembaga, membuat upaya harmonisasi secara nasional sulit dilakukan (Sigiro *et al.*, 2023).

Dari perspektif nilai dan *governance*, publik menuntut pemimpin yang memiliki kapasitas teknis memadai. Banyak yang menyuarakan bahwa pos kementerian strategis seperti Kominfo harus diisi oleh profesional, bukan politisi. Kritik ini menekankan bahwa kesalahan backup bukan hanya masalah teknologi, tapi mencerminkan kultur kerja yang permisif terhadap risiko dan korupsi anggaran. Komentar publik bahkan menyebut pengelolaan dana sebesar Rp 700 miliar untuk PDN justru diwarnai transparansi lemah dan investasi minim dalam infrastruktur keamanan yang esensial (Karnay, 2020).

SIMPULAN

Keamanan siber telah berkembang menjadi isu strategis nasional yang tidak hanya menyangkut aspek teknis, tetapi juga menyentuh dimensi kelembagaan, politik, dan kedaulatan digital negara. Melalui studi ini, dapat disimpulkan bahwa respons negara Indonesia terhadap ancaman digital masih bersifat reaktif, parsial, dan belum sepenuhnya terkoordinasi secara terpusat. Meskipun telah dibentuk lembaga khusus seperti Badan Siber dan Sandi Negara (BSSN), serta ditetapkannya sejumlah kebijakan seperti Perpres No. 47/2023 dan UU Perlindungan Data Pribadi (UU PDP), praktik di lapangan menunjukkan bahwa ketahanan siber nasional masih rapuh.

Kelemahan utama terletak pada belum meratanya penerapan standar keamanan digital antar lembaga, minimnya ketersediaan backup data yang memadai, serta keterbatasan jumlah SDM yang kompeten di bidang siber. Fragmentasi kewenangan antarinstansi juga menjadi hambatan serius dalam menciptakan sistem pertahanan digital yang terpadu. Insiden serangan ransomware terhadap pusat data nasional pada pertengahan 2024 menjadi bukti nyata bahwa infrastruktur siber negara belum memiliki sistem tanggap darurat dan mitigasi risiko yang kokoh.

Di sisi lain, upaya kolaborasi internasional, pengembangan CSIRT, dan peningkatan indeks keamanan digital menunjukkan bahwa pemerintah memiliki kesadaran terhadap urgensi masalah ini. Namun, kesadaran tersebut belum sepenuhnya diterjemahkan ke dalam tindakan struktural yang kuat dan berkelanjutan. Diperlukan reformasi menyeluruh, mulai dari desain regulasi, konsolidasi kelembagaan, peningkatan kapasitas teknis SDM, hingga penanaman budaya keamanan digital di semua level pemerintahan.

*Corresponding author
E-mail addresses: balqisfuadybsk@gmail.com

DAFTAR PUSTAKA

Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan: Jurnal Inovasi Kebijakan*, *6*(1), 1-14.

Ariel, K., Suhirwan, S., & Dohamid, A. G. (2025). Ancaman Perang Siber China terhadap Indonesia: Analisis Strategi, Dampak, dan Respons Kebijakan. *AURELIA: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia*, *4*(2), 2033-2045.

Balqish, N. Z., & Marzaman, A. P. (2025). Peran Keamanan Siber dalam Melindungi Data Kesehatan: Tanggung Jawab Negara dan Lembaga Internasional dalam Era Digital. *Triwikrama: Jurnal Ilmu Sosial*, *8*(6), 131-140.

Gani, T. A. (2023). *Kedaulatan data digital untuk integritas bangsa*. Syiah Kuala University Press.

Karnay, S. (2020). *Penerapan Electronic Government Pada Dinas Komunikasi Informatka Statistik dan Persandian Provinsi Sulawesi Selatan* (Doctoral dissertation, Universitas Hasanuddin).

Sigiro, F. H., Runturambi, A. J. S., & Widiawan, B. (2023). Collaborative Sharing Intelijen Ancaman Pada Komunitas Csirt Dalam Memperkuat Keamanan Siber Nasional. *Syntax Literate; Jurnal Ilmiah Indonesia*, *7*(9).

Simorangkir, A., Sihombing, H., Sihite, P. I., & Parhusip, J. (2024). Ransomware pada Data PDN Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber. *JOURNAL SAINS STUDENT RESEARCH*, *2*(6), 324-331.

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 7.