**Jurnal Riset Rumpun Ilmu Sosial, Politik dan Humaniora**
**Volume. 5 Nomor. 1 Januari 2026**
e-ISSN: 2828-7622; p-ISSN: 2828-7630, Hal 872-882
DOI: https://doi.org/10.55606/jurrish.v5i1.8471
*Tersedia:* https://prin.or.id/index.php/JURRISH

# Peran Badan Siber dan Sandi Negara (BSSN) dalam Arsitektur Keamanan Siber Indonesia

**Hesti Rosdiana[1*], Reja[2], Bintang Hafizh Setiawan [3]**
[1,3] Program Studi Hubungan Internasional, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
[2] Program Studi Ilmu Politik, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
**Penulis Korespondensi: hesti.rosdiana@upnvj.ac.id*

***Abstract.*** *This paper reviews the dynamics of cybersecurity in Indonesia, focusing on the role of the Indonesian National Cyber and Crypto Agency (BSSN) in Indonesia's cybersecurity architecture. The conceptual framework used is cyber security to analyze cybersecurity phenomena in Indonesia and multi-level cybersecurity governance as a tool for analyzing the role of BSSN in the field of cybersecurity. A descriptive qualitative approach is the main methodological approach in this study. With this approach, this study attempts to describe the role of BSSN in Indonesia's cybersecurity architecture. Data collection was carried out through a literature study obtained from BSSN's main documents, official reports, and related journal articles. The findings show that BSSN has a strategic role in Indonesian cybersecurity. This strategic role is demonstrated by BSSN's various achievement in cybersecurity, such as the drafting of a national cybersecurity bill, the development of human resources capacity in the cyber field and the establishment of cooperation with various parties, both domestically and internationally.*

***Keywords****: BSSN; Cyber Governance; Cybersecurity Architecture; Cybersecurity; Indonesia.*

**Abstrak**. Tulisan ini mengulas tentang dinamika keamanan siber di Indonesia, dengan fokus pada peran Badan Siber dan Sandi Nasional (BSSN) Indonesia dalam arsitektur keamanan siber Indonesia. Kerangka konseptual yang digunakan ialah keamanan siber untuk menganalisis fenomena keamanan siber di Indonesia dan tata kelola keamanan siber berbasis multi-level sebagai alat analisis peran BSSN dalam bidang keamanan siber. Pendekatan kualitatif deskriptif menjadi pendekatan metodologi utama dalam penelitian ini. Dengan pendekatan tersebut, penelitian ini berupaya mendeskripsikan peran BSSN dalam arsitektur keamanan siber Indonesia. Pengumpulan data dilakukan dengan studi pustaka yang di dapat dari dokumen utama BSSN, laporan resmi dan artikel jurnal yang terkait. Hasil temuan menunjukkan bahwa BSSN memiliki peran strategis dalam hal keamanan siber Indonesia. Peran strategis ini ditunjukkan dengan berbagai pencapaian BSSN dalam hal keamanan siber, seperti penyusunan draft keamanan siber nasional, pengembangan kapasitas sumber daya manusia di bidang siber, hingga pembentukan kerja sama dengan berbagai pihak, baik di level domestik maupun internasional.

**Kata kunci**: Arsitektur Keamanan Siber; BSSN; Indonesia; Keamanan Siber; Tata Kelola Siber

## 1. LATAR BELAKANG

Dalam beberapa dekade terakhir, beberapa isu internasional kontemporer banyak mewarnai analisis Hubungan Internasional. Dunia yang berada dalam tatanan system multipolar memberikan tantangan signifikan, tidak hanya pada aktor-aktor Hubungan Internasional yang kian bervariasi tapi juga isu-isu kontemporer yang dihadapi. Salah satu isu yang kini menjadi perhatian masyarakat global ialah isu ancaman siber. Isu ini mulai berkembang pesat pasca pandemi Covid-19, yang mana pada masa ini masyarakat global 'dipaksa' untuk tidak lepas dari ruang siber dalam kehidupan sehari-hari. Hal ini disebabkan oleh keterbatasan sosialiasi secara fisik yang diakibatkan dari adanya Covid-19.

Ruang siber telah menjadi ruang yang melekat dalam kehidupan sehari-hari masyarakat global. Sejalan dengan hal itu, berbagai tantangan mulai bermunculan, terutama ialah ancaman siber yang menuntut negara-negara global memiliki pertahanan siber yang baik. Pertahanan siber diperlukan mengingat ancaman siber yang berkembang telah bertransformasi dari sekedar

*Naskah Masuk: 18 November 2025; Revisi: 15 Desember 2025; Diterima: 29 Januari 2026; Terbit: 31 Januari 2026*

gangguan teknis menjadi instrument geopolitik dan ekonomi yang mengancam keamanan nasional suatu negara. Tahun 2023 menjadi tahun krusial bagi keamanan siber global. Tingginya ketergantungan masyarakat global pada teknologi dalam kehidupan sehari-hari mengakibatkan risiko siber menjadi bagian yang terpisahkan dari geopolitik di tahun 2023. (Forum, 2026)

Indonesia sebagai negara yang menempati urutan keempat di dunia dengan pertumbuhan pengguna internet memiliki kerentanan yang tinggi akan ancaman siber. Berdasarkan data terbaru, ancaman siber yang menargetkan Indonesia menunjukkan tren peningkatkan yang signifikan. Ini dapat dilihat dari adanya 1,2 milyar insiden serangan siber di tahun 2023 dan 6 juta kasus pada kuartal pertama di tahun 2024. (Rudiyanto, 2025) Serangan siber tersebut menargetkan sektor-sektor kritis di Indonesia, seperti perbankan dan Fintech, *E-Commerce*, Kesehatan dan pemerintah, baik itu di level pusat maupun daerah. Serangan siber juga memberikan kerugian ekonomi yang tinggi, misalnya di tahun 2023, Indonesia dilaporkan menerima kerugian moneter sebesar 10 triliun rupiah akibat serangan ransomware. (Isro' Kurniawan Rahakbauw, 2024) Sementara, data dari pemerintah di bulan November 2024 hingga Januari 2025, kerugian finansial yang diterima oleh pemerintah sebesar 476 milyar rupiah dan terdapat 1,2 juta laporan penipuan hingga pertengah tahun 2025. (Komdigi, 2025)

Dengan demikian, Indonesia memerlukan komitmen yang kuat untuk dapat menanggulangi atau sekedar meminimalisir ancaman siber yang terus terjadi. Dengan kata lain, pembangunan keamanan siber menjadi langkah utama Indonesia dalam merespon ancaman siber yang ada. Perluasan ruang siber harus masuk ke dalam lanskap geopolitik Indonesia sebagai satu kesatuan dari lanskap geopolitik yang sudah ada yakni darat, laut dan udara.

Komitmen kuat Indonesia dalam merespon ancaman siber diwujudkan melalui berbayai upaya seperti penguatan regulasi dan literasi digital, pengembangan dan pemanfaatan teknologi, juga pembentukan institusi khusus untuk persoalan siber yaitu Badan Siber dan Sandi Negara (BSSN). BSSN merupakan institusi keamanan siber nasional yang dibentuk untuk melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengkonsolidasikan seluruh pihak terkait dengan keamanan siber. BSSN dibentuk pada tahun 2017 dan bertanggung jawab langsung kepada Presiden. Pembentukan BSSN mencerminkan keseriusan pemerintah Indonesia dalam hal keamanan siber. BSSN memiliki 8 fungsi utama yang tertuang dalam pasal 3 Perpres No. 28 Tahun 2021. Dalam hal penyelenggaraan tata kerja, BSSN memiliki tanggung jawab untuk bisa bekerja sama secara baik dengan lembaga-lembaga lain yag terkait dengan urusan pemerintahan di bidang keamanan siber, seperti yang tertuang dalam Bab III Perpres No. 28 Tahun 2021 dari pasal 33

sampai dengan pasal 44. Berdasarkan hal itu, penelitian ini menganalisis peran BSSN dalam menghadapi ancaman siber sebagai ancaman transnasional. Penelitian ini juga akan melihat sejauh mana efektivitas strategi dan kebijakan BSSN dalam mitigasi ancaman siber yang menyerang Indonesia, serta melihat tantangan dan hambatan yang dihadapi BSSN dalam mitigasi tersebut.

## 2. KAJIAN TEORITIS

Penelitian ini menggunakan kerangka konseptual keamanan siber dalam perspektif Hubungan Internasional. Kajian Hubungan Internasional melihat keamanan siber sebagai upaya negara-negara dalam mengembangkan pertahanan kuat terhadap serangan siber. Pertahanan kuat tersebut dapat dibangun melalui kerja sama internasional yang berkelanjutan, berinovasi dalam teknologi pertahanan dan penetapan norma dan aturan yang jelas tentang perilaku yang dapat diterima di ruang siber. (Kumar, 2023)

Dalam kajian Hubungan Internasional, keamanan siber menjadi salah satu faktor utama dalam membentuk tatanan hubungan internasional. Oleh karenanya, kerja sama internasional menjadi hal esensial untuk membangun ketahanan negara dalam menghadapi serangan siber. Dengan kata lain, pendekatan komprehensif perlu dilakukan guna pembentukan norma-norma perilaku yang bertanggung jawab di ruang siber, mempromosikan pertukaran inf ormasi, dan mengembangkan strategi bersama pertahanan siber. (Kumar, 2023, p. 3)

Pendekatan komprehensif tersebut, dapat dilaksanakan salah satunya melalui konsep pemerintahan multi-level (*multi-level governance*). Konsep ini menekankan bahwa setiap pembuat kebijakan dari level pusat hingga daerah memiliki tanggung jawab yang berbeda untuk mendukung fokus yang sama, dalam hal ini ialah keamanan siber. konsep pemerintahan multi-level juga menekankan sinergi antara berbagai pemangku kepentingan selain pemerintah, seperti perusahaan, organisasi social dan masyarakat umum untuk pertahanan keamanan siber. (Li, 2024) Dalam hal ini, konsep pemerintahan multi-level merupakan bagian dari tata kelola keamanan siber.

Tata kelola keamanan siber merupakan kerangka kerja dan proses yang diterapkan oleh organisasi untuk mengelola risiko keamanan siber dan memastikan kepatuhan terhadap undang-undang dan peraturan. Tata kelola keamanan siber berfungsi sebagai tulang punggung manajemen risiko, menyediakan akuntabilitas, pengawasan dan keselarasan strategis antara langkah-langkah dengan tujuan organisasi. (Qudus, 2025) Tata kelola keamanan siber akan menetapkan kebijakan, tanggung jawab dan mengevaluasi kerangka kerja manajemen risiko,

yang memungkinkan rspon proaktif terhadap ancaman siber yang muncul. Konsep keamanan siber digunakan dalam penelitian ini untuk menganalisis pembentukan BSSN sebagai upaya Indonesia dalam merespon ancaman siber yang berkembang. BSSN menjadi alat utama pemerintah Indonesia dalam tata kelola keamanan sibernya.

## 3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan penelitian kualitaif deskriptif yaitu pendekatan metodologis yang memberikan ringkasan komprehensif tentang peristiwa atau pengalaman. Pendekatan ini mengadopsi pendekatan penyelidikan naturalistik, yang berkomitmen untuk mempelajarai fenomena dalam keamanan alamiah, tanpa memilih variable penelitian secara sebelumnya atau memanipulasinya. (Liebenberg, 2024) Ciri khas dari pendekatan ini ialah menciptakan gambaran umum yang sistematis, akurat, dan factual mengenai fakta, karakteristik, dan hubungan antara fenomena yang diteliti. (Furidha, 2023)

Lebih lanjut, Lienberg (2024) mengungkapkan bahwa pendekatan kualitatif deskriptif merupakan metode yang praktis dan efektif untuk mendeskripsikan pengalaman dan peristiwa manusia. Pendekatan kualitatif deksriptif memiliki kelebihan pada fleksibilitasnya yang dapat digunakan dalam berbagai konteks penelitian. Tujuan pendekatan kualitatif deskriptif adalah menyajikan ringkasan komprehensif tentang peristiwa dalam Bahasa sehari-hari, tetapi tetap dekat dengan data dan permukaan kata-kata serta peristiwa. (Liebenberg, 2024, p. 4) Pendekatan beragam dalam pengumpulan data dapat digunakan dalam studi deskriptif kualitatif. Penelitian ini menggunakan metode pengumpulan data melalui studi literatur. Studi literatur ialah pengumpulan data dengan penelusuran buku atau dokumen yang relevan dengan topik penelitian. Tujuannya adalah untuk membandingkannya atau memperoleh pemahaman yang lebih mendalam tentang temuan-temuan terkait topik penelitian. (Furidha, 2023, p. 5)

Dengan menggunakan pendekatan penelitian kualitatif deskriptif, penelitian ini berupaya memberikan gambaran tentang peran BSSN dalam menghadapi dan mengelola ancaman keamanan siber yang menyerang Indonesia sepanjang tahun 2023-2025. Penelitian ini juga berupaya mendeskripsikan tentang bagaimana ancaman keamanan siber yang ada di Indonesia dan bagaimana kolaborasi BSSN mengatasi persoalan tersebut dengan berbagai stake-holder terkait. Oleh karena itu, pengumpulan data dalam penelitian ini dilakukan dengan studi literatur yang berasal dari berbagai dokumen dan laporan resmi pemerintah Indonesia dan juga artikel jurnal atau penelitian lain yang terkait dengan topik penelitian.

## 4. HASIL DAN PEMBAHASAN

### Dinamika Ancaman Siber di Indonesia

Perkembangan teknologi komunikasi dan informasi telah mendorong Indonesia mengalami transformasi digital yang cepat di berbagai sektor seperti keuangan, kesehatan, *e-commerce*, hingga layanan pemerintah. Di sisi lain, transformasi digital membuka peluang baru untuk ancaman siber, misalnya serangan ransomware, kebocoran data hingga penipuan phishing.

Dalam beberapa tahun terakhir, Indonesia menghadapi peningkatan signifikan ancaman siber. Peningkatan ancaman siber ini disebabkan oleh tiga faktor utama yaitu pertumbuhan ekonomi digital yang pesat, rendahnya kesadaran keamanan siber dan posisi Indonesia sebagai negara rentan terhadap serangan siber. (Proxsis, 2025) Selama kurun waktu 2021-2024, Indonesia menghadapi tren ancaman siber yang bervariasi. Pada tahun 2021, BSSN mengungkapkan Indonesia menghadapi sekitar 1,6 milyar serangan siber. Sebagian besar serangan siber yang ditemukan ialah jenis *Malware*, yang kemudian disusul oleh *Trojan Activity* dan *Information Gathering*. (Rahmawati, 2022) Insiden serangan siber menunjukkan penurunan di tahun 2022, yang mana menurut BSSN insiden serangan siber yang dihadapi oleh Indonesia mencapai hamper 1 milyar. Salah satu hal yang menjadi sorotan dari insiden siber di tahun 2022 adalah kasus peretasan dan kebocoran data. Pada awal tahun 2022, Indonesia menerima peretasan di website pemerintah dan kebocoran data lebih dari 130GB yang diklaim dari Bank Indonesia dan dijual oleh pelaku kejahatan siber Bjorka.

Untuk tahun 2023, serangan siber yang menyerang Indonesia tercatat berjumlah sekitar 279,84 juta. Artinya, di tahun 2023, Indonesia mengalami penurunan angka serangan siber sebesar 24,4% dibandingkan dengan tahun sebelumnya. (Firman, 2024) Jenis serangan siber yang terjadi di tahun 2023 mencakup phishing, malware dan Distribute Denial of Service (DDoS). Akan tetapi, di tahun 2024, laporan BSSN memperlihatkan adanya kenaikan serangan siber di Indonesia sekitar 1,01%. Jumlah serangan siber berkisar pada angka 609,39 juta. Dari berbagai insiden serangan siber yang terjadi di tahun 2024, terdapat satu peristiwa yang menjadi perhatian serius yakni Ketika serangan ransomware menyerang Pusat Data Nasional (PDN) pada Juni 2024. Serangan ini berdampak secara nyata pada berhentinya layanan pemerintah hingga kerentanan infrastruktur nasional terhadap musuh siber. Dua bulan kemudian, serangan siber menyerang Badan Kepegawaian Negara (BKN) yang mengalami kebocoran data lebih dari 4,7 juta. (IndosecSummit, 2025)

Keragaman dan intensitas ancaman siber yang ada di Indonesia, menunjukkan beberapa hal yang perlu dikaji oleh pemerintah Indonesia. Pertama, kompleksitas dan keragaman ancaman siber yang menyerang Indonesia memperlihatkan bahwasanya Indonesia adalah negara yang memiliki kerentanan tinggi terhadap serangan siber, namun masih lemah dalm hal ketahanan sibernya. Menurut data dari situs *National Cyber Security Index* (NCSI), Indonesia berada pada peringkat ke-49 dari total 176 negara, dengan skor keamanan siber mencapai 63,64 poin. (Pratomo, 2024) Artinya, Indonesia memerlukan penguatan keamanan siber dengan teknologi dan sumber daya manusia berkualitas untuk bisa mengatasi serangan siber yang terjadi.

Kedua, berbagai insiden serangan siber yang terjadi menunjukkan bahwa Indonesia memerlukan regulasi dan norma-norma hukum yang lebih mengikat untuk mengatasi serangan siber. Indonesia memiliki dasar hukum yang mengatur keamanan siber tertuang dalam UU ITE Nomor 19 Tahun 2016. UU ITE mencakup aturan untuk beberapa pelanggaram yang terjadi di ranah siber dan memberikan perlindungan hukum untuk konten system elektronik dan transaksi elektronik. Akan tetapi, UU ITE belum mencakup aspek penting dalam hal keamanan siber. Ketiga, Indonesia perlu melakukan upaya komprehensif dengan berbagai pemangku kepentingan untuk penguatan keamanan siber. Salah satu hal yang dapat dilakukan untuk mewujudkan hal ini adalah dengan penguatan peran BSSN.

**Peran BSSN Dalam Lanskap Keamanan Siber Indonesia**

Selama beberapa dekade terakhir, pemerintah Indonesia telah membuat undang-undang dan regulasi dasar untuk mengatasi berbagai ancaman siber yang ada, seperti kejahatan siber, perlindungan data dan transaksi elektronik. Pemerintah juga telah mendorong kolaborasi antara otoritas regulasi dan bisnis untuk memperkuat postur keamanan siber negara. (Law, 2025) Selain itu, Indonesia juga membentuk lembaga yang secara khusus untuk menangani persoalan siber, yaitu BSSN.

BSSN ialah lembaga yang dibentuk oleh pemerintah Indonesia pada tahun 2017 melalui keputusan Presiden. Dalam operasinya, BSSN masuk ke dalam kerangka Kementerian Koordinator Bidang Urusan Politik, Hukum dan Keamanan yang melaporkan langsung kepada Presiden. Kepala BSSN memiliki empat wakil yang bertanggung jawab atas identifikasi dan deteksi ancaman, perlindungan, respons, dan pemulihan serta kebijakan teknis untuk pemantauan pengendalian.

BSSN dibentuk sebagai pengganti Badan Kriptografi Nasional dan memiliki lima tujuan dalam strategi keamanan sibernya, yaitu ketahanan siber, keamanan layanan public, penegakan hukum siber, budaya keamanan siber dan keamanan siber dalam ekonomi digital.

(BSSN, 2020) Tujuan ini termasuk untuk mempromosikan keterlibatan multi-pemangku kepentingan dan membangun kepercayaan global terhadap pengelolaan ruang siber Indonesia. (Studies, 2021) Salah satu implementasi dari tujuan tersebut dapat dilihat pada rilis draf strategi keamanan siber yang dilakukan oleh BSSN pada Desember 2020. Perilisan draft strategi keamanan siber berfokus pada insiden siber yang signifikan secara nasional.

Kehadiran BSSN sebagai lembaga penanganan siber berperan dalam menjalin koordinasi dan kerja sama antara institusi dan pemangku kepentingan lainnya di bidang siber. Koordinasi dan kerja sama ini dilakukan bersama dengan institusi pemerintah dalam negeri yang terkait dan juga dengan aktor-aktor lain di luar pemerintahan Indonesia. Sejak pembentukannya BSSN telah melakukan banyak hal dalam penanganan keamanan siber Indonesia. Pada tahun 2019 misalnya, BSSN menginisiasi diskusi public dan symposium nasional RUU tentang Keamanan dan Ketahanan Siber dan mengusulkan RUU Persandaian dan RUU Rahasia Negara dalam Program Legislasi Nasional Pemerintah tahun 2020-2024. Pada tahun yang sama, BSSN juga membentuk Gov-CSIRT (*Government Computer Security Incident Response Team*) dengan misi mengkoordinasikan dan mengelaborasi layanan keamanan siber di sektor pemerintah dan membangun kapasitas sumber daya keamanan siber pada sektor pemerintah. (Haryanto, 2023)

BSSN juga memiliki prioritas dalam hal pengembangan kompetensi SDM di bidang keamanan siber sebagai bagian dari penguatan ketahanan digital menghadapi ancaman siber. Pengembangan kompetensi SDM tidak hanya dilakukan di internal BSSN saja, tapi juga di lingkungan eksternal, yang mencakup kementerian/lembaga, pemerintah daerah dan institusi lainnya. Selama kurun waktu 2021-2024, BSSN telah menghasilkan 814 lulusan dalam pelatihan pengembangan SDM di bidang keamanan siber, baik internal maupun eksternal BSSN. (Dewangga, 2025) Selain itu, BSSN juga rutin menggelar pelatihan strategis bagi Penyelenggaran Sistem Elektronk (PSE) di lingkup publik.

Peran BSSN dalam penguatan keamanan siber Indonesia juga dilaksanakan dengan berkolaborasi menjalin kerja sama dengan berbagai pihak. Dalam beberapa tahun terakhir, BSSN dengan gencar membuka kerja sama baik di level domestik (bersama kementerian/Lembaga) maupun di level internasional (dengan negara atau organisasi internasional). Pada Oktober 2025 misalnya, BSSN memperkuat kerja sama dengan Kementerian Pertanian di bidang keamanan siber guna memastikan system pertanian digital Indonesia beroperasi denga naman dan efisien di tengah transformasi teknologi. (News, 2025)

Selain itu, BSSN juga menjalin kerja sama strategis bersama LKPP pada Mei 2025 dan Kemenko PMK di tahun 2021.

Sementara di level internasional, BSSN telah menjalin kerja sama dengan Australia di bidang keamanan siber pada tahun 2018. Kerja sama tersebut diimplementasikan dengan melaksanakan *cyber boot camp, cyber policy workshop, cyber business connection* dan *cyber policy dialogue*. (Magrisa, 2020) Pada tahun yang sama, Indonesia juga menandatangani kerja sama dengan Belanda. Implementasi kerja sama tersebut ditunjukkan dengan penyelenggaraan dialog keamanan siber yang memuat pemecahan permasalahan siber dan penguatan kapasitas dan hukum siber di Indonesia. Selain itu, BSSN juga memperkuat kerja sama di bidang siber dengan Korea Selatan, melalui kerja sama BSSN dan *Korea Internet and Security Agency* (KISA) di tahun 2022. Lalu, dengan Inggris yang sudah berjalan sejak tahun 2018, namun di dalam beberapa tahun terakhir mengalami perkembangan signifikan dalam kerja saman, juga dengan Malaysia di tahun 2025. Di level regional, BSSN gencar mendorong ASEAN untuk mekanisme penanganan siber secara regional dan melalui forum ASEAN, BSSN memperkuat diplomasi sibernya dengan mitra internasional.

Berbagai upaya BSSN yang dilakukan BSSN mencerminkan peran strategis Lembaga ini dalam penguatan keamanan siber Indonesia. Dalam konsep tata Kelola keamanan siber berbasis multi-level, BSSN sebagai lembaga yang relatif baru mampu memperlihatkan kinerjanya secara baik yang ditunjukkan dengan berbagai pencapaiannya baik mulai dari pembuatan draft keamanan siber, diskusi tentang keamanan siber, pengembangan kompetensi sumber daya manusia di bidang siber hingga beragam jalinan kerja sama dengan berbagai pemangku kepentingan.

Dengan kata lain, BSSN berfungsi sebagai *central coordinating authority* yang menjembatani interaksi antara level nasional, sectoral dan actor non negara dalam pengelolaan risiko siber. Secara vertical, BSSN telah menunjukkan upayanya dalam membangun standarisasi dan konsistensi kebijakan lintas level pemerintahan melalui penyusunan dokumen kebijakan dan draft regulasi keamanan siber nasiol. Sementara di level horizontal, BSSN aktif mendorng koordinasi lintas sector melalui forum diskusi keamana siber, pengembangan kapasitas sumber daya manusia di bidang siber dan penguatan kerja sama dengan berbagai pihak. Hal ini berarti BSSN menjalankan prinsip *multi-stakeholder engagement* dalam tata kelola keamanan siber. Dengan demikian, peran BSSN dalam arsitektur keamanan siber Indonesia dapat dipahami sebagai proses yang masih bersifat dinamis, dan masih memerlukan penguatan koordinasi dan konsolidasi dengan berbagai pemangku kepentingan guna mewujudkan arsitektur keamanan siber nasional yang efektif dan berkelanjutan.

## 5. KESIMPULAN DAN SARAN

Ancaman siber adalah isu yang tengah menjadi prioritas oleh negara-negara di seluruh dunia, tidak terkecuali Indonesia. Masalah ancaman siber Indonesia dalam beberapa tahun terakhir memperlihatkan kondisi yang mengkhawatirkan. Berdasarkan data dan laporan resmi dari BSSN, ancaman siber di Indonesia menunjukkan tingkat kerentanan yang tinggi dengan berbagai variasi ancamannya. Ini berdampak serius pada pelayanan digital publik Indonesia yang banyak mendapati gangguan akibat adanya serangan siber. Serangan siber juga menyebabkan kebocoran data yang mengancam perlindungan data nasional masyarakat Indonesia. Pendekatan komprehensif diperlukan untuk mengatasi ancaman siber.

Sebagai respon ancaman siber, pemerintah Indonesia telah membentuk badan yang secara khusus menangani masalah keamanan siber. BSSN adalah badan yang dibentuk secara khusus untuk mengatasi keamana siber Indonesia. Sejak awal pembentukannya, BSSN diberikan tugas yang dalam pelaksanaannya memerlukan koordinasi dan konsolidasi dengan berbagai pemangku kepentingan. Berdasarkan analisis tata Kelola keamanan siber, penelitian ini memperlihatkan BSSN memiliki peran strategis sebagai aktor sentral dalam penguatan keamanan siber nasional Indonesia. Dengan fungsi koordinatif dan regulatif, BSSN tidak hanya berperan dalam penyusunan kebijakan dan norama keamanan siber nasional Indonesia, tapi juga menjadi akomodir dalam interaksi antara berbagai level pemerintahan dan pemangku kepentingan lainnya.

## DAFTAR REFERENSI

Forum, W. E. (2026). *Global cybersecurity outlook 2026*. World Economic Forum.

Furidha, B. W. (2023). Comprehension of the descriptive qualitative research method: A critical assessment of the literature. *ACITYA WISESA: Journal of Multidisciplinary Research*, 2(4), 1–8. https://doi.org/10.56943/jmr.v2i4.443

Haryanto, S. M. (2023). Upaya peningkatan keamanan siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) tahun 2017–2020. *Global Political Studies Journal*, 7(1), 56–69. https://doi.org/10.34010/gpsjournal.v7i1.8141

Isro' Kurniawan Rahakbauw, I. A. (2024). Analisis potensi ancaman siber pada bidang ekonomi. *Jurnal Kajian Stratejik Ketahanan Nasional*, 1–13.

Kumar, D. R. (2023). Cyber security in international relations. *International Journal of Advanced Research*, 1–8.

Li, J. (2024). Multi-governance model of new cybercrime under the risk of new technologies: Risks and responses. In *2nd International Conference on Global Politics and Socio-Humanities* (pp. 21–29). Lecture Notes in Education Psychology and Public Media. https://doi.org/10.54254/2753-7048/2024.BO17965

Liebenberg, S. H. (2024). Qualitative description as an introductory method to qualitative research for master's-level students and research trainees. *International Journal of Qualitative Methods*, 1–4.

Magrisa, D. (2020). Kerja sama Badan Siber dan Sandi Nasional (BSSN) Indonesia dengan Department of Foreign Affairs and Trade (DFAT) Australia dalam pengembangan cyber security. *JOM FISIP*, 1–11.

Qudus, L. (2025). Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges. *International Journal of Science and Research Archive*, 14(1), 1146–1163. https://doi.org/10.30574/ijsra.2025.14.1.0225

Rudiyanto, A. P. (2025). Defending the nation in the cyber era: Indonesia's response to non-military security threats. *Enrichment: Journal of Multidisciplinary Research and Development*, 3(9), 3521–3532. https://doi.org/10.55324/enrichment.v3i9.555

The International Institute for Strategic Studies. (2021). *Cyber capabilities and national power: A net assessment*. The International Institute for Strategic Studies.

Badan Siber dan Sandi Negara. (2020, December 14). *BSSN organization*. https://cloud.bssn.go.id/s/

Rahmawati, D. (2022, March 7). BSSN temukan 1,6 miliar serangan siber sepanjang 2021, mayoritas malware. *detikNews*. https://news.detik.com/berita/d-5972491/bssn-temukan-1-6-miliar-serangan-siber-sepanjang-2021-mayoritas-malware

Firman, M. N. (2024, February 2). Data jumlah serangan cyber di Indonesia tahun 2023. *Widya Security*. https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/

Pratomo, G. P. (2024, July 5). Hacker Brain Cipher minta Indonesia sadar cybersecurity, seberapa lemah keamanan? *Kompas*. https://tekno.kompas.com/read/2024/07/05/09030087/hacker-brain-cipher-minta-indonesia-sadar-cybersecurity-seberapa-lemah-keamanan

Makarim & Taira S. (2025, January). *Staying secure: Key updates on Indonesia's cybersecurity law* (Issue 2). https://www.makarim.com/storage/uploads/b3e30663-57c2-4679-aca8-f705adb8b99e/Issue-2---January-2025---MT-Advisory---Staying-Secure-Key-Updates-on-Indonesia's-Cybersecurity-Law.pdf

Dewangga, O. S. (2025, January 2). BSSN siapkan ribuan SDM untuk hadapi serangan siber. *Rakyat Merdeka*. https://rm.id/baca-berita/government-action/249486/bssn-siapkan-ribuan-sdm-untuk-hadapi-serangan-siber

Indosec Summit. (2025, March 24). The escalating cyber threat in Indonesia: A wake-up call for digital security. https://indosecsummit.com/the-escalating-cyber-threat-in-indonesia-a-wake-up-call-for-digital-security/

Proxsis Group. (2025, June 11). Tren ancaman siber di Indonesia meningkat: Berikut fakta yang harus diketahui. https://it.proxsisgroup.com/tren-ancaman-siber-di-indonesia-meningkat-berikut-fakta-yang-harus-diketahui/

Kementerian Komunikasi dan Digital. (2025, August 8). Kejahatan siber capai kerugian Rp 476 M, AI diperkuat untuk cegah ancaman di ruang digital. https://www.komdigi.go.id/berita/siaran-pers/detail/kejahatan-siber-capai-kerugian-rp-476-m-ai-diperkuat-untuk-cegah-ancaman-di-ruang-digital

Antara News. (2025, October 5). Ministry, BSSN collaborate to bolster cybersecurity in agriculture. https://en.antaranews.com/news/385125/ministry-bssn-collaborate-to-bolster-cybersecurity-in-agriculture