Jurnal Impresi Indonesia (JII)
p-ISSN: 2828-1284 e-ISSN: 2810-062x
Vol. 5. No. 3. 2026

Analisis Kebijakan Keamanan Siber Indonesia dalam Strategi Nasional Keamanan Siber

Idden Aryasatya*, Stanislaus Riyanta, Eko Daryanto
Universitas Indonesia
Email: iddenaryasatya0101@gmail.com*

Keywords:
Cybersecurity;
National Cybersecurity Strategy (SNKS);
Cyber Resilience;

Abstract

Background: *This research analyzes Indonesia's cybersecurity policy through the Assumption Analysis approach and cyber resilience theory, with a focus on the implementation of the 2023 National Cyber Security Strategy (SNKS).* ***Objective:*** *This research compares Indonesia's preparedness with Malaysia's, which shows better performance in data governance and protection.* ***Methods:*** *The analysis in this paper will be based on retrospective policy analysis and cyber resilience theory to dissect the implications of cybersecurity in Indonesia.* ***Results:*** *Key findings indicate that Indonesia faced several serious cyber incidents between 2021 and 2025, including a ransomware attack on the National Data Center and a data breach involving the National Health Insurance (BPJS Kesehatan) program. Although the National Cyber Security System (SNKS) has been launched, its implementation remains largely normative and not yet operational. Issues such as overlapping authority, minimal incident reporting, and digital inequality weaken national cyber resilience.* ***Conclusion:*** *This study recommends the establishment of an independent cross-sectoral institution, mandatory incident reporting, adoption of international standards such as NIST, strengthening cyber human resources, and policy integration with the ASEAN Cybersecurity Cooperation Framework 2025. The transition to a proactive cyber resilience paradigm is a strategic necessity in facing increasingly complex digital threats.*

Kata Kunci:
Keamanan Siber;
Strategi Nasional Keamanan Siber (SNKS);
Ketahanan Siber;

Abstrak

Latar belakang: Penelitian ini menganalisis kebijakan keamanan siber Indonesia melalui pendekatan Assumption Analysis dan teori ketahanan siber, dengan fokus pada implementasi Strategi Nasional Keamanan Siber (SNKS) 2023. **Tujuan:** Studi ini membandingkan kesiapan Indonesia dengan Malaysia, yang menunjukkan capaian lebih baik dalam tata kelola dan perlindungan data. **Metode:** Analisis dalam makalah ini akan didasarkan pada analisis kebijakan retrospektif dan teori ketahanan siber untuk membedah implikasi keamanan siber di Indonesia. **Hasil:** Temuan utama menunjukkan bahwa Indonesia menghadapi berbagai insiden siber serius pada periode 2021–2025, termasuk serangan ransomware terhadap Pusat Data Nasional dan kebocoran data BPJS Kesehatan. Meski SNKS telah diluncurkan, pelaksanaannya masih bersifat normatif dan belum operasional. Permasalahan seperti tumpang tindih otoritas, minimnya pelaporan insiden, dan ketimpangan digital memperlemah ketahanan siber nasional. **Kesimpulan:** Studi ini merekomendasikan pembentukan lembaga independen lintas sektor, wajibnya pelaporan insiden, adopsi standar internasional seperti NIST, penguatan SDM siber, serta integrasi kebijakan dengan Kerangka Kerja Sama Keamanan Siber ASEAN 2025. Transisi menuju paradigma ketahanan siber proaktif menjadi kebutuhan strategis dalam menghadapi ancaman digital yang semakin kompleks.

PENDAHULUAN

Di era digital saat ini, ketersediaan sebagian besar kemajuan teknologi, baik itu komunikasi, pengarsipan data, keuangan, dll, telah menjadi dominan melekat pada aktivitas manusia. Sebaliknya, jenis teknologi yang digunakan dalam banyak kasus sangat terkait dengan Internet of Things (IoT), istilah yang diciptakan pada tahun 1991 yang mengklasifikasikan IoT sebagai teknologi yang sedang berkembang dengan banyak kemungkinan, banyak kemajuan yang diberikannya juga disertai dengan kekurangan yang dapat terbukti merugikan privasi atau keselamatan seseorang (Legal, 2024). Peretasan, masalah pengawasan, serta masalah privasi telah menjadi atribut yang menentukan dari kekurangan teknologi yang ada, dengan demikian muncul gagasan tentang "janji versus risiko" (Ait Mouha, 2021). Penelitian ini mengamati masalah tersebut melalui lensa keamanan makro, karena topik itu sendiri membahas analisis kebijakan dalam keamanan siber nasional Indonesia dan infrastrukturnya.

Keamanan siber Indonesia dinilai masih kurang jika dibandingkan dengan negara-negara tetangga di Asia Tenggara. Di tingkat internasional, Indonesia berada di peringkat 83 dari 160 negara, sedangkan di kawasan Asia Tenggara, Indonesia berada di peringkat 4 dengan skor Indeks Keamanan Siber Nasional (NCSI) 63,64 dari 100. Sebagai perbandingan, Malaysia berada di peringkat pertama dengan skor 79,22 (NCSI, 2022). Meskipun infrastruktur digital telah hadir di Indonesia, namun pertumbuhannya dibarengi dengan berbagai masalah yang menunjukkan kurangnya fondasi fundamental, seperti kesenjangan digital dan masalah keamanan siber (Ait Mouha, 2021; Ardiansyah & Nugroho, R. A., 2024; UMY, 2024). Sementara itu, pesatnya perluasan infrastruktur digital juga menimbulkan risiko kerentanan data, serangan siber, dan keterbatasan infrastruktur. Meskipun kesadaran akan masalah keamanan siber sudah ada, kerangka hukum yang ada di Indonesia, yaitu Undang-Undang Informasi dan Transaksi Elektronik, masih perlu terus diperbarui untuk mengatasi kompleksitas dan kerapuhan keamanan siber (ICLG, 2024). Indonesia mengalami sejumlah serangan siber besar antara tahun 2024 dan 2025. Serangan ransomware terhadap Pusat Data Nasional pada bulan Juni 2024 menyebabkan masalah pada layanan dan operasi imigrasi di bandara-bandara besar. Serangan ini memengaruhi 44 departemen pemerintah, termasuk Kementerian Imigrasi dan Kementerian Koordinator Investasi (Reuters, 2024). Selain itu, pada awal tahun 2025, komplotan ransomware DragonForce mengincar PT PINS Indonesia, yang merupakan anak perusahaan PT Telkom Indonesia. Hal ini menyebabkan data-data penting perusahaan dipublikasikan di web gelap (CYFIRMA, 2025).

Seiring dengan kondisi dunia maya dan keamanan Indonesia, ketahanan Indonesia untuk tetap bertahan pasca berbagai peristiwa atau guncangan menjadi suatu keniscayaan. Kebocoran data BPJS Kesehatan misalnya yang terjadi pada tahun 2021 telah berdampak pada 279 juta warga negara, peristiwa ini akan menjadi studi kasus yang perlu dibedah dan dikaji lebih mendalam karena merupakan salah satu kasus yang sangat dibutuhkan keamanan data di Indonesia (Sari, 2021). Selain itu, BSSN (Badan Siber dan Sandi Negara) di Indonesia telah mengeluarkan Strategi Nasional Keamanan Siber yang memberikan informasi yang cukup mengenai penguatan dan kesiapan keamanan siber Indonesia. Strategi Nasional Keamanan Siber tidak hanya menyebutkan berbagai macam ancaman yang ada dalam keamanan siber, tetapi juga memberikan strategi yang menggambarkan terciptanya ekosistem keamanan siber yang mumpuni yang meliputi regulasi, teknologi, sumber daya manusia, dan kerja sama dalam

dan luar negeri (BPK RI, 2020). Oleh karena itu, makalah ini akan membahas regulasi dan strategi Indonesia, sekaligus menyampaikan pemahaman tentang keamanan siber sebagai dimensi baru dalam pertahanan negara.

Mengenai dasar penelitian ini adalah komparatif, skala antar negara akan memberikan akurasi dan wawasan yang bermakna, dengan demikian studi kasus akan membandingkan keamanan siber Indonesia dengan Malaysia, masing-masing peringkat keempat dan pertama dalam NCIS. Menurut NCSI (2023), keamanan siber Indonesia lebih buruk daripada Malaysia, peringkat ketiga di ASEAN dan ke-49 secara global saat itu. Malaysia mendapat peringkat lebih tinggi di sektor ini karena pelaksanaan kebijakan yang lebih unggul (Infobankstore, 2023). Malaysia telah menerapkan sistem yang lebih ketat untuk mendaftarkan pengguna data, yang lebih melindungi data pribadi karena pengawasan pemerintah yang ketat. Indonesia saat ini tidak memilikinya (ResearchGate, 2024). Menurut penelitian, Malaysia mengambil pendekatan yang lebih proaktif untuk mengalokasikan sumber daya keamanan siber dan mengembangkan peraturan daripada Indonesia, yang memiliki organisasi yang terfragmentasi dan kekurangan sumber daya. Akibatnya, Indonesia saat ini menjadi negara yang paling sering menjadi sasaran serangan siber di Asia Tenggara. Ini berarti bahwa infrastruktur keamanan sibernya harus segera ditingkatkan sekarang (Indosecsummit, 2024).

Berdasarkan penelitian terdahulu yang berjudul " **Tantangan Hukum Terhadap Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia** " oleh Fadhila Rahman Najwa (2024). Penelitian ini mengevaluasi efektivitas kerangka hukum Indonesia dalam menangani kejahatan siber, menyoroti tantangan implementasi dan perlunya peningkatan kapasitas penegakan hukum. Disamping artikel, " **Tinjauan Kritis Urgensi Penguatan Implementasi Keamanan dan Ketahanan Siber di Indonesia** " oleh Indirwan, Sarah Safira Aulianisa (2020) dalam Lex Scientia Law Review, Vol. 4, No. 1. Penelitian ini menyoroti rendahnya peringkat Indonesia dalam indeks keamanan siber global dan tantangan implementasi kebijakan terkait. Faktor utamanya adalah kurangnya koordinasi antarlembaga dan terbatasnya regulasi teknis. Rekomendasi utamanya adalah pembentukan undang-undang khusus tentang keamanan siber dan peningkatan koordinasi antarlembaga untuk memperkuat ketahanan siber nasional. Dan sebuah literatur " **Strategi Keamanan Siber Indonesia: Permasalahan dan Tantangan** " oleh Arief Isdiman Saleh & Muhammad Danu Winata (2023) dalam Prosiding International Joint Conference on Arts and Humanities. Penelitian ini membahas strategi keamanan siber Indonesia, mengidentifikasi tantangan seperti regulasi yang tumpang tindih, kurangnya sumber daya manusia, dan pengabaian hak asasi manusia. Meskipun ada regulasi penting seperti UU ITE dan UU Perlindungan Data Pribadi, tantangannya semakin kompleks dengan meningkatnya penggunaan internet. Rekomendasi utama adalah memperkuat kerja sama internasional dan meningkatkan kesadaran publik tentang pentingnya keamanan siber.

Penelitian ini menawarkan kebaruan akademik dalam lima aspek utama. Pertama, menggunakan pendekatan Assumption Analysis William Dunn secara sistematis (identifikasi aktor, asumsi, perbandingan, pengelompokan, sintesis) yang belum pernah diterapkan dalam kajian keamanan siber Indonesia. Kedua, mengintegrasikan teori ketahanan siber OJK (deteksi, respons, pemulihan, adaptasi) ke dalam analisis kebijakan nasional. Ketiga, melakukan analisis komparatif mendalam dengan Malaysia berbasis data 2020-2025 dan mengaitkannya dengan Kerangka ASEAN 2025. Keempat, memetakan secara sistematis 18 sumber data sekunder dari

berbagai perspektif untuk memberikan gambaran holistik ekosistem keamanan siber nasional. Kelima, merumuskan lima rekomendasi kebijakan strategis berbasis analisis asumsi, standar global NIST, penguatan SDM siber, dan harmonisasi regional ASEAN. Penelitian ini mengisi kesenjangan literatur sekaligus memberikan kontribusi praktis bagi pengembangan kebijakan keamanan siber Indonesia yang proaktif, terintegrasi, dan berkelanjutan.

Terkait ketahanan siber Indonesia, Indonesia telah menyoroti sejumlah isu seperti peringkat keamanan siber global yang rendah, kerangka hukum yang tidak memadai, dan kurangnya kesiapan kelembagaan dalam menangani insiden siber. Padahal, BSSN, sebagaimana disebutkan sebelumnya, bersama dengan Strategi Nasional Keamanan Siber (SNKS) No.47 2023 umumnya bersifat normatif dan belum sepenuhnya mengimplementasikan konsep ketahanan dalam kerangka analitis (Pemerintah Republik Indonesia, 2023). Untuk mengisi kesenjangan tersebut, penerapan teori ketahanan siber, dari kerangka teori keamanan siber Otoritas Jasa Keuangan (OJK) dalam konteks keamanan nasional mungkin terbukti penting, karena teori tersebut bersifat multidisiplin dan mencakup banyak aspek dalam keamanan siber beserta cara kerjanya.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis faktor-faktor yang berkontribusi terhadap keamanan siber dengan memanfaatkan teori ketahanan siber, sekaligus membandingkannya dengan kebijakan SNKS yang dikeluarkan oleh BSSN. Sebaliknya, penelitian ini akan mencoba memberikan wawasan yang lebih mendalam tentang keamanan siber dan infrastruktur digitalnya, terutama tentang bagaimana ia bereaksi terhadap guncangan dan peristiwa tertentu, selain bagaimana ia berpotensi pulih.

METODE PENELITIAN

Analisis dalam makalah ini akan didasarkan pada analisis kebijakan retrospektif dan teori ketahanan siber untuk membedah implikasi keamanan siber di Indonesia. Aspek retrospektif dianalisis melalui data terkini yang merupakan kebijakan SNKS, karena kebijakan tersebut merupakan pembahasan utama dalam makalah ini, dan bertujuan untuk melihat kebijakan sebagaimana adanya dan bagaimana kebijakan tersebut beroperasi, sekaligus memberikan evaluasi, analisis deskriptif, dan potensi perbaikan dalam kebijakan tersebut.

Data yang dikumpulkan akan sepenuhnya merupakan informasi sekunder dan diolah menjadi kualitatif dengan data kuantitatif untuk memberikan fakta dan akurasi. Karena penelitian ini menggunakan data sekunder, informasi dikumpulkan dari berbagai artikel dan dokumen hukum yang membahas SNKS dan menganalisis isinya sambil membandingkannya dengan sejumlah penelitian yang berkorelasi dengan keamanan siber. Sebaliknya, data yang diperoleh akan diolah melalui analisis curah pendapat melalui upaya jawaban potensial dan memberikan saran terhadap kebijakan saat ini. Dengan demikian, pengumpulan data hanya berupaya untuk membuktikan kemanjuran SNKS tentang bagaimana kebijakannya memengaruhi sistem keamanan siber di Indonesia.

Selain pengolahan data kualitatif analisis kebijakan menggunakan kerangka teori oleh William N. Dunn akan digunakan. Analisis asumsi, menurut Dunn (2018), adalah metode analisis yang dimaksudkan untuk menggabungkan asumsi-asumsi yang saling bertentangan yang berkaitan dengan masalah kebijakan. Analisis asumsi terdiri dari lima tahap. Ini adalah sebagai berikut:

1. Identifikasi aktor kebijakan. Pada tahap ini, aktor kebijakan diidentifikasi, ditingkatkan, dan diberi prioritas berdasarkan penilaian seberapa besar pengaruh dan pengaruh aktor tersebut terhadap proses kebijakan;
2. Penghasilan asumsi. Pada tahap ini, peneliti mengumpulkan sumber data dan gagasan yang mendasari rekomendasi yang diberikan oleh aktor kebijakan terkait kebijakan;
3. Membandingkan asumsi: Pada tahap ketiga, peneliti secara sistematis membandingkan, mengontraskan, dan mengevaluasi rekomendasi serta asumsi-asumsi yang mendasarinya;
4. Mengelompokkan asumsi: Pada tahap ini, asumsi-asumsi yang telah diuji pada tahap sebelumnya dikelompokkan berdasarkan tingkat kepentingannya bagi masing-masing aktor kebijakan;
5. Mensintesis asumsi: Pada tahap terakhir ini, peneliti menggabungkan asumsi-asumsi yang telah diuji pada tahap terakhir ini.

Tabel 1. Sumber Data Penelitian

No.	Tanggal	Judul	Sumber
1	12-11-2020	Tinjauan Kritis Implementasi Ketahanan Keamanan Siber di Indonesia	https://lexscientia.com/ojs/index.php/lslr/article/view/123
2	22-02-2021	Kesenjangan Digital dan Keterbatasan Infrastruktur di Indonesia	https://www.worldbank.org/id/negara/indonesia/publikasi/laporan-kesenjangan-digital-di
3	23-05-2021	Data BPJS Kesehatan Diduga Bocor: Dukungan Penuntasan	https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas
4	31-12-2022	Indeks Keamanan Siber Nasional Indonesia 2022	https://ncsi.ega.ee/negara/id_2022/
5	17-10-2022	Undang-Undang Perlindungan Data Pribadi Indonesia	https://peraturan.bpk.go.id/Detail/231592/uu-no-27-tahun-2022
6	20-01-2023	Undang-Undang Perlindungan Data Pribadi 2010 (Malaysia)	https://www.pdp.gov.my/jpdpv2/assets/act/Personal%20Data%20Protection%20Act%202010.pdf
7	15-03-2023	Peraturan dan Undang-Undang Keamanan Siber Indonesia 2024	https://iclg.com/bidang-praktik/undang-undang-dan-peraturan-keamanan-siber/indonesia
8	15-07-2023	Keamanan Siber Indonesia Peringkat 5 ASEAN	https://infobankstore.com/artikel/1175/keamanan-siber-indonesia-peringkat-ke-5-di-asean-di-bawah-malaysia-dan-filipina
9	30-08-2023	Strategi Keamanan Siber Indonesia: Tantangan Kelembagaan	https://www.researchgate.net/publication/376543123_Permasalahan_dan_Tantangan_Strategi_Keamanan_Siber_di_Indonesia
10	04-09-2023	Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional	https://peraturan.bpk.go.id/Detail/255542/perpres-no-47-tahun-2023

11	13-02-2024	Mengapa Keamanan Siber Indonesia Perlu Segera Ditingkatkan?	https://www.indosecsummit.com/keamanan-siber-di-indonesia-perlu-peningkatan-cepat-yang-paling-di-targetkan-di-kawasan/
12	10-03-2024	Laporan Tahunan BSSN 2023: Lanskap Ancaman Siber	https://www.bssn.go.id/uploads/laporan_tahunan_2023.pdf
13	14-05-2024	Kebijakan Keamanan Siber Nasional Malaysia 2024	https://www.cybersecurity.my/id/tentang_kami/strategi/strategi_keamanan_cyber_nasional
14	01-06-2024	Perbandingan Indeks Keamanan Siber: Indonesia vs. Malaysia	https://www.researchgate.net/figure/Perbandingan-Indeks-Keamanan-Siber-dengan-Malaysia_tbl4_364267812
15	26-06-2024	Lebih dari 40 lembaga di Indonesia terkena serangan siber di pusat data	https://www.reuters.com/world/asia-pacific/lebih-dari-40-lembaga-indonesia-dilanda-serangan-cyber-pusat-data-2024-06-26/
16	03-07-2024	Kerangka Kerjasama Keamanan Siber ASEAN 2025	https://asean.org/wp-content/uploads/2024/07/ASEAN-Cybersecurity-Cooperation-Framework-2025.pdf
17	05-09-2024	Kerangka Ketahanan Siber untuk Infrastruktur Kritis	https://www.nist.gov/publications/kerangka-keamanan-siber-infrastruktur-kritis
18	31-01-2025	Laporan Intelijen Mingguan – Ransomware DragonForce menargetkan PT PINS Indonesia	https://www.cyfirma.com/berita/laporan-intelijen-mingguan-31-jan-2025/

Sumber: Hasil Inventarisasi Literatur (2020-2025)

Rentang Waktu Penelitian (2020-2025) dengan fokus pada periode implementasi SNKS 2020. Jangkauan penelitian:

1. Periode 2020-2025 sesuai permintaan
2. Termasuk kasus ransomware terbaru tahun 2025 (No. 2)
3. Kebocoran data historis (No. 3) untuk analisis longitudinal

Semua sumber dipilih berdasarkan kriteria:

1. Relevansi dengan kebijakan SNKS 2020-2024
2. Data komparatif Indonesia-Malaysia
3. Cakupan aspek ketahanan siber (ketahanan siber)
4. Keterbaruan (2021-2025)
5. Keragaman perspektif (pemerintah, akademik, lembaga internasional)

HASIL DAN PEMBAHASAN

Penelitian ini menyajikan analisis mendalam terhadap ketahanan dan keamanan bahasa siber nasional Indonesia dengan berlandaskan 18 sumber data sekunder sebagaimana tercantum dalam Tabel 1 Analisis ini Dilakukan secara sistematis dengan menggunakan pendekatan *Assumption Analysis* yang dikembangkan oleh William Dunn dalam kerangka analisis kebijakan publik. Pendekatan ini memungkinkan Identifikasi menyeluruh terhadap

permasalahan, pengembangan ide strategis, dan penyusunan kebijakan berdasarkan data empiris dan teoritis yang dikumpulkan melalui telaah literatur, dokumentasi, dan laporan kebijakan.

Hasil dari penelitian menunjukkan bahwa Indonesia mengalami berbagai insiden siber serius pada jarak waktu 2021–2025. Salah satu insiden paling mencolok adalah serangan ransomware pada Pusat Data Nasional yang berdampak lebih banyak dari 40 lembaga negara, termasuk lembaga vital seperti Direktorat Jenderal Imigrasi dan Kementerian Investasi. Insiden ini menyebabkan kelumpuhan layanan umum selama beberapa hari dan menciptakan kekacauan administrasi dalam pengurusan dokumen kewarganegaraan dan perjalanan. Selain itu, kasus kebocoran data yang melibatkan BPJS Kesehatan pada tahun 2021 menjadi titik kembali penting yang ditunjukkan kelemahan sistem pengamanan data negara. Kasus tersebut menyebabkan data pribadi 279 juta warga negara Indonesia diduga tersebar ke forum gelap dan dieksploitasi untuk berbagai Kejahatan digital seperti pencurian identitas, penipuan keuangan, dan phishing.

Serangan lain yang terjadi pada awal tahun 2025 melibatkan grup ransomware internasional yang menyasar PT PINS Indonesia— anak perusahaan dari BUMN PT Telkom Indonesia. Data internal perusahaan tersebar dan didistribusikan di dark web, menunjukkan bahwa bahkan perusahaan dengan kemampuan teknologi tinggi pun tidak luput dari ancaman digital jika tidak dilindungi oleh sistem keamanan dan tata kelola risiko yang solid.

SKSN sebagaimana diatur dalam Perpres No. 47 Tahun 2023 menjadi dokumen kerangka strategis utama dalam penguatan keamanan siber Indonesia. Namun, dokumen tersebut dinilai masih terlalu normatif dan belum memuat langkah-langkah operasional yang dapat diimplementasikan secara langsung oleh instansi evaluasi teknis. kerangka hukum menunjukkan bahwa meskipun Indonesia sudah memiliki UU Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), pelaksanaannya masih belum optimal. Terjadi tumpang berdekatan Kewenangan antara Kementerian Komunikasi dan Informatika, BSSN, serta polisi yang menimbulkan ketidakefisienan dan kebingungan dalam penanganan insiden siber.

Sebagai pembanding, Malaysia tampil jauh lebih progresif dalam hal regulasi dan kelembagaan saudara. UU Perlindungan Data Pribadi 2010 memberikan kerangka hukum yang kuat untuk perlindungan data warga negara dan pengguna layanan digital. Selain itu, lembaga CyberSecurity Malaysia (CSM) aktif dalam melakukan audit, pemantauan, edukasi publik, dan peningkatan kapasitas SDM. Sistem pelaporan kejadian di Malaysia juga lebih transparan dan memiliki sanksi yang mengikat, yang mendorong entitas publik dan swasta untuk Membatasi data keamanan.

Perbedaan dasar antara negara kedua juga terlihat dalam alokasi sumber daya dan keseriusan kebijakan publik. Malaysia memiliki strategi yang lebih terkoordinasi dan berbasis risiko, dengan investasi signifikan dalam pelatihan SDM dan pengembangan kebijakan teknis yang komprehensif. Sementara itu, Indonesia masih menunjukkan ketergantungan pada pendekatan sektoral dan reaktif, serta belum memiliki kebijakan tunggal yang terintegrasi semua pemangku minat di bidang keamanan perbedaan siberi ini diperparah oleh rendahnya belanja keamanan siber nasional Indonesia dibandingkan dengan laju pertumbuhan digital ekonominya.

Ketimpangan Lainnya terletak pada kesiapan Teknisi dan tanggap darurat terhadap kejadian. Ketika Malaysia telah menetapkan prosedur tetap di tengah tanggapan nasional yang aktif, Indonesia masih Bergantung pada koordinasi ad hoc dan laporan Ketahanan. Ketiadaan standar teknis yang menarik juga menyulitkan harmonisasi kebijakan antar lembaga. Hal ini bercermin dalam peringkat NCSI, di mana Malaysia mencetak skor Tertinggi di ASEAN, sementara Indonesia masih tertinggal secara signifikan. Ketimpangan ini memperlihatkan perbedaan dalam efektivitas kebijakan serta Konsistensi dalam penerapan strategi keamanan digital.

Analisis atas Laporan Tahunan Badan Siber dan Sandi Negara menampilkan peningkatan jumlah serangan, terutama pada sektor pemerintahan dan infrastruktur kritis. Serangan yang dominan antara lain phishing, malware, dan ransomware yang menyasar agen dengan kelemahan dalam sistem keamanan berbasis jaringan. Sayangnya, laporan tersebut masih bersifat deskriptif dan belum disertai rencana tindakan konkret. Beberapa Sastra akademis juga mengkritik bahwa strategi keamanan siber indonesia cenderung administratif dan tidak responsif terhadap dinamika ancaman yang berkelanjutan berkembang.

Masalah juga muncul dari sisi keterwakilan digital. Masih banyak wilayah terpencil di Indonesia belum memiliki akses internet yang layak, apalagi infrastruktur perlindungan siber. Hal ini membuat wilayah-wilayah tersebut rentan terhadap serangan digital tanpa Adanya kapasitas lokal untuk melakukan mitigasi. Ketimpangan digital juga menciptakan perbedaan literasi digital, yang mengecewakan risiko karena rendahnya Pemahaman masyarakat terhadap praktik keamanan siber dasar.

Lebih lanjutnya, ketahanan siber tidak hanya ditentukan oleh aspek teknis, namun juga ditentukan oleh kualitas sumber daya manusia. Berdasarkan kerangka dari OJK tentang ketahanan siber pada sektor perbankan, ketahanan digital ditentukan oleh kemampuan lembaga untuk mencegah, mendeteksi, merespons, dan memulihkan diri dari serangan siber. Jika prinsip ini diterapkan dalam konteks nasional, maka dapat lanjutan bahwa lembaga umum seperti BPJS belum mencapai standar ketahanan minimum karena kelemahannya kemampuan deteksi awal dan lambatnya proses pemulihan pasca-insiden.

Indonesia juga perlu memperkuat keterlibatannya dalam pekerjaan sama regional. Kerangka Kerjasama Keamanan Siber ASEAN 2025 mendorong kolaborasi lintas negara dalam hal pemantauan insiden, pertukaran informasi, dan harmonisasi regulasi. Indonesia dapat bermain peran lebih aktif sebagai inisiator dalam membangun protokol keamanan bersama dan interoperabilitas sistem pertahanan siber ASEAN.

Berikut dibawah ini adalah visualisasi dari analisis hasil data dengan analisis kebijakan penelitian Dunn (*Assumption Analysis*).

Tabel 2. Tabel Analisis Asumsi Kebijakan Siber Nasional Indonesia (SNKS)

No	Daftar Aktor Kebijakan	Pernyataan Aktor sebagai Dasar Asumsi	Kategorisasi Asumsi	Pengelompokan Asumsi Berdasarkan Tingkat Kepentingan
1	BSSN	SNKS memperkuat ketahanan siber melalui koordinasi lintas sektor dan pembentukan standar	Regulasi, Keamanan Nasional, Kelembagaan	Tinggi - Penentu utama arah kebijakan dan implementasi nasional

		regulatif serta pengawasan teknis insiden		
2	Kominfo	Fokus utama adalah penguatan literasi digital, pemerataan infrastruktur jaringan, serta penyuluhan masyarakat mengenai perlindungan data pribadi	SDM, Infrastruktur, Edukasi Siber	Tinggi - Pelaksana kebijakan publik dan jembatan antara masyarakat dan teknologi
3	DPR RI	Mendesak perlunya pembaruan hukum melalui pembuatan UU Siber Nasional karena UU ITE dianggap terlalu umum dan tidak cukup mengatur kerentanan baru	Legislasi, Tata Kelola, Pengawasan	Tinggi - Penentu kerangka hukum dan anggaran negara
4	PT Telkom Indonesia	Dunia usaha dan BUMN perlu jaminan regulasi serta pedoman teknis standar dalam mengelola sistem keamanan data dan mitigasi risiko	Industri, Teknologi, Investasi	Tinggi - Infrastruktur digital strategis nasional yang berperan langsung dalam pengendalian data
5	ID-CERT & CISSReC	Sistem pelaporan wajib insiden keamanan siber serta audit mandiri oleh lembaga independen diperlukan untuk menciptakan transparansi dan perbaikan berkelanjutan	Teknologi, Respons Insiden, Transparansi	Sedang - Aktor teknis non-pemerintah yang menjembatani dengan masyarakat
6	Akademisi (UI, UGM)	Regulasi masih normatif dan tumpang tindih; dibutuhkan tata kelola kelembagaan baru dan pendekatan berbasis riset serta evaluasi longitudinal	Evaluasi, Ilmu Pengetahuan, Reformasi Institusional	Sedang - Kontributor wacana dan inovasi kebijakan
7	CyberSecurity Malaysia	Indonesia tertinggal dalam sistem pelaporan insiden dan belum menerapkan mekanisme insentif/sanksi seperti Malaysia yang memperkuat kepatuhan digital	Komparatif, Regional, Efektivitas Kebijakan	Sedang - Referensi strategis dalam pemetaan kelemahan nasional
8	ASEAN-CSF	Harmonisasi kebijakan siber antar negara Asia Tenggara penting untuk mendorong interoperabilitas dan kesiapan kolektif terhadap serangan regional	Kerja Sama Regional, Diplomasi Siber	Rendah - Tekanan eksternal strategis, namun bukan prioritas teknis nasional saa

Sumber: Hasil Analisis Data Primer (2025) dengan Pendekatan Assumption Analysis Dunn (2018)

Tabel 2 menunjukkan hasil analisis asumsi terhadap kebijakan keamanan siber nasional—khususnya SNKS—yang dilakukan. Dalam konteks ini, aktor-aktor kebijakan diidentifikasi berdasarkan peran mereka dalam membuat, menerapkan, dan mengevaluasi

kebijakan keamanan siber Indonesia. Misalnya, BSSN adalah otoritas utama pengarah SNKS dan bertanggung jawab untuk memperkuat undang-undang dan menciptakan standar nasional untuk pengamanan infrastruktur digital yang sangat penting bagi negara. BSSN juga membuat peta jalan keamanan digital, yang mencakup cara mencegah, mendeteksi, menanggapi, dan memperbaiki ancaman siber yang terus meningkat.

Selain BSSN, Kominfo sangat penting untuk meningkatkan literasi digital, mengelola infrastruktur komunikasi, dan memberikan informasi publik tentang solusi dan ancaman siber. Selain itu, kominfo berfungsi sebagai penghubung antara pemerintah dan masyarakat, terutama dalam menyusun program edukasi digital untuk seluruh Indonesia, termasuk wilayah tertinggal. Karena kebutuhan mendesak untuk merevisi atau mengganti UU ITE dengan UU khusus keamanan siber yang lebih relevan dengan masalah teknologi saat ini, DPR RI, melalui fungsi legislasinya, juga memainkan peran penting. Mereka bertanggung jawab untuk menciptakan landasan hukum yang akan melindungi hak digital warga dan memperjelas wewenang lembaga.

Organisasi lain seperti PT Telkom Indonesia dan komunitas keamanan siber seperti ID-Computer Emergency Response Team (CERT) dan Communication and Information System Security Research Center "CISSReC" membantu meningkatkan sisi teknis dan memantau insiden. Sebagai pengelola infrastruktur digital skala nasional dan sebagai perusahaan swasta yang paling rentan terhadap ancaman siber, tugas Telkom sangat penting. Komunitas teknis independen tidak hanya menawarkan pemantauan alternatif, tetapi juga memainkan peran penting dalam pembentukan sistem peringatan dini berbasis komunitas yang lebih fleksibel dan responsif. Menurut analisis ini, aktor kebijakan memiliki tingkat kepentingan dan kontribusi yang berbeda, tetapi mereka semuanya merupakan bagian dari ekosistem yang harus saling mendukung untuk membangun ketahanan digital yang menyeluruh dan berkelanjutan di negara ini. Dalam menghadapi kompleksitas ancaman digital global, pendekatan kolaboratif lintas aktor menjadi kunci untuk menghasilkan strategi yang lebih kuat dan terukur.

Tabel 3. Pengelompokan Asumsi

Asumsi Utama	Regulasi	Infrastruktur & SDM	Sosial	Teknologi & Industri	Regionalisme
Perbedaan	Fragmentasi kewenangan antara BSSN, Kominfo, dan Polri dalam penanganan insiden siber	Keterbatasan akses infrastruktur di daerah 3T (tertinggal, terdepan, terluar), rendahnya literasi digital	Belum semua kelompok masyarakat memahami pentingnya keamanan digital	Tidak ada standar teknis yang seragam antar sektor; swasta masih enggan berinvestasi besar	Indonesia belum maksimal harmonisasi kebijakan dengan ASEAN CSF 2025
Persamaan	Kebutuhan UU Siber Nasional sebagai landasan hukum terpadu	Perlunya pelatihan dan sertifikasi siber berbasis OJK dan NIST (National Institute of Standards and Technology)	Perlu edukasi publik dan kampanye literasi siber	Audit keamanan dan early warning system berbasis industri	Dukungan prinsip kerja sama kawasan melalui ASEAN CSF

Sumber: Hasil Sintesis Analisis Data (2025)

Tabel 3 menunjukkan pergeseran pendapat para aktor kebijakan mengenai arah kebijakan keamanan siber nasional dan menyertakan perbedaan dan persamaan. Dalam konteks perbedaan, asumsi-asumsi seperti fragmentasi kelembagaan, kesenjangan infrastruktur di wilayah 3T, kurangnya kesadaran masyarakat tentang keamanan digital, dan kurangnya harmonisasi regional dan standar teknis menjadi perhatian utama. Fragmentasi lembaga seperti BSSN, Kominfo, dan kepolisian menyebabkan kebingungan dalam koordinasi dan respons terhadap insiden. Ini menunjukkan bahwa pihak berwenang menyadari berbagai tantangan struktural yang menghambat kinerja SNKS dan menimbulkan ancaman terus menerus terhadap stabilitas digital bangsa.

Sebaliknya, kebutuhan mendesak untuk membuat Undang-Undang Siber Nasional yang menyeluruh dan komprehensif muncul, yang merupakan proposal konstruktif dalam konteks ini. Kerangka hukum yang tidak konsisten akan diselesaikan dengan undang-undang ini. Itu juga akan menetapkan sanksi dan insentif yang berlaku untuk semua entitas digital, baik publik maupun swasta. Rekomendasi tambahan termasuk meningkatkan kemampuan SDM di sektor siber melalui pelatihan dan sertifikasi keamanan siber berbasis standar internasional seperti OJK dan NIST. Selain itu, dibutuhkan sistem audit keamanan dan pelaporan insiden yang wajib, terutama untuk sektor infrastruktur penting seperti energi dan layanan publik.

Selain itu, pentingnya mendukung ASEAN Cybersecurity Cooperation Framework 2025 menunjukkan bahwa beberapa pihak berusaha untuk mencapai keselarasan kebijakan regional. Pengembangan kerja sama internasional akan memungkinkan pertukaran informasi intelijen siber, koordinasi lintas batas, dan pengembangan sistem interoperabilitas. Tabel ini secara keseluruhan menunjukkan bagaimana kebijakan berubah dari reaktif menjadi proaktif dan beradaptasi dengan kemajuan teknologi dan kebutuhan perlindungan digital masyarakat. Teori-teori ini menekankan betapa pentingnya negara untuk membangun ekosistem digital yang aman, terbuka, dan berkeadilan walaupun dengan adanya berlawanan pikiran atau pendapat.

Tabel 4. Pengelompokan Asumsi Berdasarkan Tingkat Kepentingan

Kategori Asumsi	Perbedaan	Persamaan	Kesimpulan
Regulasi	BSSN, Kominfo, dan Polri belum satu suara; tumpang tindih otoritas memperlambat respons	Seluruh aktor sepakat pentingnya UU Siber Nasional sebagai pijakan hukum utama	Perlu segera penataan regulasi lintas lembaga agar tidak kontraproduktif
SDM & Infrastruktur	Daerah tertinggal (3T) masih jauh dari literasi dan infrastruktur digital yang memadai	Sertifikasi SDM, pelatihan, dan inklusi digital menjadi kebutuhan bersama	Perlu strategi nasional yang fokus pada pemerataan dan pembiayaan jangka panjang
Teknologi & Industri	Perusahaan swasta belum memiliki insentif untuk berinvestasi dalam sistem keamanan	Audit dan sistem pelaporan wajib dianggap perlu oleh semua pihak	Negara harus memberikan stimulus fiskal atau insentif bagi dunia usaha
Sosial	Rendahnya kesadaran publik menyebabkan kerentanan pengguna terhadap penipuan digital	Kampanye dan edukasi publik diakui penting untuk semua lapisan masyarakat	Media, sekolah, dan organisasi masyarakat sipil harus digandeng lebih erat
Regionalisme	Belum ada roadmap implementasi regional	ASEAN-CSF dianggap acuan	Indonesia harus mulai mengintegrasikan strategi nasional dengan kebijakan regional

dari pihak pemerintah Indonesia	penting bagi pembaruan kebijakan

Sumber: Hasil Sintesis Analisis Data (2025)

Tabel 4 membagi asumsi berdasarkan kategori kebijakan dan menjelaskan perbedaan, persamaan, dan implikasi masing-masing kategori. Terdapat perbedaan di bidang hukum karena lembaga seperti BSSN, Kominfo, dan polisi tidak bekerja sama dengan baik, yang menyebabkan kebingungan dan fragmentasi dalam penanganan insiden. Upaya mitigasi dan respons cepat terhambat oleh kurangnya kerangka kerja yang kuat. Namun, semua pihak setuju bahwa UU Siber Nasional diperlukan untuk membuat dasar hukum yang jelas yang menjamin wewenang yang jelas, peran yang jelas, dan penegakan hukum yang efektif.

Semua orang setuju bahwa daerah tertinggal menghadapi tantangan yang signifikan dalam literasi dan akses ke infrastruktur digital, yang menyebabkan perbedaan siber yang signifikan antara kota besar dan wilayah pinggiran dalam hal sumber daya manusia dan infrastruktur. Namun, semua pihak setuju bahwa, agar setiap orang dapat berpartisipasi dalam sistem keamanan digital nasional, pelatihan, sertifikasi, dan inklusi digital adalah kebutuhan strategis yang harus dipenuhi. Selain itu, ini mencakup menyediakan pelatihan jarak jauh, membangun laboratorium digital, dan menyediakan dukungan perangkat untuk sekolah di daerah 3T.

Aktor swasta dalam teknologi dan industri menunjukkan bahwa peraturan dan insentif diperlukan untuk menerapkan sistem keamanan yang kuat. Ini termasuk pengakuan praktik terbaik industri, keringanan pajak untuk investasi dalam keamanan TI, dan perlindungan hukum untuk pelaporan insiden. Pelaporan insiden yang terbuka dan transparan sangat penting untuk pembuatan kebijakan berbasis bukti. Solusi bersama yang inklusif harus mencakup kampanye publik, memasukkan masalah keamanan digital ke dalam kurikulum sekolah, dan melibatkan komunitas lokal dalam advokasi digital, karena kurangnya literasi siber masyarakat di bidang sosial.

Walaupun belum sepenuhnya dimasukkan ke dalam kebijakan nasional, ASEAN CSF 2025 mulai dianggap sebagai rencana masa depan yang penting. Ini menunjukkan jenis regionalisme yang berbeda. Sangat penting bagi negara-negara Asia Tenggara untuk menyelaraskan kebijakan keamanan digital mereka karena ancaman siber tidak mengenal batas geografis. Indonesia akan memiliki akses ke mekanisme bantuan teknis, pertukaran pengetahuan, dan dukungan diplomatik dalam kasus serangan lintas negara dengan berpartisipasi dalam inisiatif ASEAN. Secara keseluruhan, seperti yang ditunjukkan oleh analisis dalam tabel ini, keberhasilan SNKS memerlukan pendekatan yang berfokus pada integrasi, jangka panjang, dan lintas sektor. Metode ini harus menggabungkan kebijakan nasional dengan komitmen global untuk membangun ekosistem digital yang aman, adaptif, resilient, dan berdaulat di tengah ancaman global yang semakin kompleks.

Dengan memanfaatkan pendekatan *Assumption Analysis* dari Dunn dan analisis teori OJK, serta didukung oleh seluruh sumber data yang dimiliki dikaji secara komprehensif, penelitian ini menyimpulkan bahwa Indonesia berada pada titik kritis dalam pembangunan sistem ketahanan siber nasional. Transisi dari paradigma keamanan siber (reaktif) menuju ketahanan siber (proaktif dan adaptif) adalah keharusan mutlak di era transformasi digital.

Paradigma baru ini akan menentukan kemampuan negara dalam menjaga Stabilitas, keamanan data, dan kepercayaan umum terhadap institusi digital di masa depan.

Pembahasan

BSSN dibentuk untuk mengamankan infrastruktur digital Indonesia dan menunjukkan komitmen negara terhadap keamanan siber nasional. SNKS 2020 menguraikan tujuan kebijakan BSSN, yang meliputi pengembangan sistem pertahanan siber yang tangguh untuk menangkal serangan di bidang pertahanan, energi, dan komunikasi. BSSN bertujuan untuk meningkatkan ketahanan siber negara dengan menyatukan pemerintah, akademisi, dan sektor swasta. Badan tersebut juga bermaksud untuk memperkuat respons negara terhadap peristiwa siber dan menyediakan enkripsi untuk layanan digital penting. Hal ini menunjukkan pergeseran pendekatan dari pertahanan reaktif menjadi pertahanan antisipatif (Widodo, 2020; Yusuf & Syaifulloh, 2020; Putri, 2024).

Namun, posisi Indonesia dalam NCSI masih lebih rendah dibandingkan negara-negara lain di kawasan tersebut, termasuk Malaysia. Menurut data terbaru, Malaysia secara konsisten menempati peringkat lebih tinggi dalam hal persiapan, undang-undang, dan kerangka kelembagaan. Ada beberapa penjelasan untuk perbedaan ini: Malaysia mendirikan badan keamanan siber profesional seperti CyberSecurity Malaysia sejak awal, memimpin penerapan kebijakan, dan menyelenggarakan kegiatan sektor publik dan swasta. Sebaliknya, Indonesia telah berjuang dengan fragmentasi kelembagaan dan persetujuan legislatif yang lambat, sehingga sulit untuk melakukan perluasan kapasitas yang cepat (Yusuf & Syaifulloh, 2020; Tan, 2023).

SNKS 2020 merupakan langkah positif bagi Indonesia karena menyediakan cetak biru untuk menyelaraskan rencana dan mengoordinasikan kebijakan. Namun, kesenjangan antara strategi dan implementasi masih menjadi masalah utama. Indonesia harus mengatasi duplikasi birokrasi dan memastikan bahwa sumber daya digunakan dengan tepat untuk mengembangkan kemampuan sibernya. Studi perbandingan menunjukkan bahwa negara-negara dengan kerangka kerja keamanan siber terpusat dan investasi berkelanjutan dalam literasi digital mengungguli negara-negara dengan sistem yang terfragmentasi. Hal ini terbukti dari kontras antara Malaysia dan Indonesia (Putri, 2024; Rahman, 2023).

Keamanan siber merupakan komponen penting ketahanan nasional, terutama karena infrastruktur digital merupakan fondasi bagi industri-industri penting seperti perbankan, transportasi, dan kesehatan masyarakat. Ketahanan dalam konteks keamanan nasional mencakup lebih dari sekadar kemampuan untuk menanggapi serangan. Ketahanan juga mencakup kemampuan untuk beradaptasi, memulihkan diri, dan terus beroperasi dalam menghadapi bahaya yang terus berlanjut. Keamanan siber kini menjadi komponen penting ketahanan, yang berarti risiko harus terus dipantau, strategi ketahanan harus dikembangkan, dan lembaga-lembaga harus berkolaborasi (Widodo, 2020; Gunawan & Lee, 2023).

Salah satu tantangan utama dalam mengimplementasikan SNKS di Indonesia adalah rendahnya kolaborasi aktif antara sektor publik dan sektor swasta, khususnya dalam berbagi informasi mengenai insiden siber. Banyak perusahaan enggan melaporkan insiden keamanan karena kekhawatiran reputasi atau kurangnya kejelasan hukum terkait pelaporan tersebut. Di negara-negara maju seperti Amerika Serikat dan Inggris, pelaporan insiden sudah menjadi kewajiban yang dilindungi oleh undang-undang, serta disertai dengan insentif untuk meningkatkan transparansi (Rahardjo, 2022; Effendy et al., 2023). Kurangnya sistem pelaporan

insiden yang solid di Indonesia menyebabkan terbatasnya data yang dapat digunakan untuk analisis risiko nasional dan strategi pertahanan yang berbasis bukti (Pratama, 2021). Padahal, kemampuan untuk memprediksi dan menanggapi ancaman secara efektif sangat bergantung pada data yang tersedia dan kecepatan pelaporannya.

Selain itu, masih terdapat tantangan dalam membangun budaya keamanan digital (cyber hygiene) di tingkat individu dan organisasi. Meskipun literasi digital semakin ditekankan, sebagian besar kampanye masih bersifat sporadis dan belum terintegrasi dalam kurikulum pendidikan nasional secara menyeluruh (Hasibuan, 2023). Di negara seperti Estonia dan Korea Selatan, pendidikan keamanan siber telah masuk sejak pendidikan dasar, memperkuat pemahaman masyarakat sejak dini akan pentingnya perlindungan data pribadi dan ancaman dunia maya (Ardiansyah & Nugroho, 2024). Indonesia perlu mencontoh model ini untuk membangun ketahanan jangka panjang melalui penguatan kapasitas individu, bukan hanya melalui pendekatan kelembagaan dan teknologi. Jika pendekatan kultural dan edukatif tidak diperkuat, maka strategi teknis dan regulatif dalam SNKS tidak akan berdampak optimal.

Terakhir, peningkatan keamanan siber Indonesia sangat penting untuk mencapai tujuan yang lebih besar, yakni kedaulatan digital dan ketahanan nasional. Seiring berkembangnya ancaman siber, kita harus melakukan lebih dari sekadar meningkatkan sistem kita. Kita juga perlu menciptakan masyarakat yang sadar akan ancaman siber, merencanakan masa depan, dan berkolaborasi dengan negara lain. Indonesia mungkin hanya dapat mengejar ketertinggalan dari negara-negara tetangganya dan mempertahankan dunia sibernya jika mengambil tindakan ini (Tan, 2023; Gunawan & Lee, 2023).

Rekomendasi Kebijakan

Lima rekomendasi kebijakan strategis utama dibuat setelah 18 sumber data yang relevan dan dapat diandalkan dievaluasi. Rekomendasi ini bertujuan untuk meningkatkan secara menyeluruh dan berkelanjutan keamanan siber nasional Indonesia dan tata kelolanya. Pertama, disarankan untuk membentuk lembaga lintas sektor yang mandiri di seluruh negeri untuk menangani keamanan siber. Lembaga ini harus diberi kewenangan penuh untuk melakukan penyelidikan, audit keamanan, dan pemulihan pasca-serangan untuk memastikan respons cepat dan terkoordinasi terhadap setiap insiden siber. Aspen Institute (2024) menyarankan model kebijakan keamanan nasional modern, yang menekankan betapa pentingnya otoritas yang independen dan profesional dalam keamanan digital. Struktur organisasi ini sejalan dengan model ini.

Kedua, sangat penting bagi organisasi publik maupun swasta untuk melaporkan pelanggaran siber. Kebijakan ini perlu didukung oleh sistem yang memberikan insentif dan sanksi administratif untuk pelaporan yang cepat dan transparan. CISA (2024) menyatakan bahwa sistem pelaporan yang baik merupakan bagian penting dari manajemen risiko siber nasional. Ketiga, disarankan agar kerangka kerja NIST diadopsi secara menyeluruh di semua sektor yang relevan untuk meningkatkan kapasitas prosedural dan teknis untuk melindungi infrastruktur penting seperti penerbangan, energi, dan layanan kesehatan. Menurut Cynet (2025), kerangka NIST telah terbukti berhasil meningkatkan ketahanan terhadap serangan berbasis sistem dan jaringan yang kompleks.

Keempat, strategi jangka panjang bergantung pada penguatan sumber daya manusia dalam keamanan siber. Pemerintah harus mendukung program pelatihan, pendidikan formal, dan sertifikasi profesional berbasis standar nasional seperti yang ada di industri jasa keuangan

dan TI. KBI (2024) menyatakan bahwa kualitas dan ketersediaan tenaga kerja siber yang terampil sangat penting untuk mengidentifikasi dan merespons ancaman secara proaktif. Kelima, untuk memperkuat posisi Indonesia dalam lanskap digital Asia Tenggara, sangat penting untuk menyelaraskan kebijakan keamanan siber domestik dengan inisiatif kerja sama regional ASEAN. Menurut Kaspersky 2024, kerja sama ini akan memungkinkan pembentukan standar kerja sama, pengakuan sistem pertahanan siber satu sama lain, dan mekanisme kerja sama dalam menghadapi ancaman siber global yang semakin kompleks.

KESIMPULAN

Untuk menyimpulkan, sejumlah besar masalah yang masih dihadapi sistem keamanan siber Indonesia menghambat kinerja pertahanan digital negara. Implementasi SNKS menghadapi banyak hambatan, termasuk kelembagaan yang fragmentasi, regulasi yang ketat, literasi digital yang rendah, dan kurangnya koordinasi lintas sektor. Jika dibandingkan dengan Malaysia, strategi Indonesia masih reaktif, sedangkan Malaysia menggunakan pendekatan yang lebih terorganisir dan berbasis risiko. Untuk membangun sistem yang tangguh, Indonesia harus beralih ke paradigma ketahanan siber yang proaktif, berbasis data, dan kolaboratif lintas pemangku kepentingan, menurut evaluasi menyeluruh yang melibatkan pendekatan "analisis asumsi" dan teori ketahanan OJK.

Studi ini, yang didasarkan pada 18 sumber data sekunder dan studi perbandingan kebijakan, menekankan betapa pentingnya membuat UU Siber Nasional, membuat lembaga independen lintas sektor, dan meningkatkan kerja sama regional dalam ASEAN CSF 2025. Selain itu, rekomendasi strategis termasuk upaya untuk menciptakan budaya keamanan digital melalui pendidikan anak-anak, pelaporan insiden yang wajib, dan insentif untuk sektor swasta. Oleh karena itu, Indonesia harus menerapkan pendekatan regulatif, teknis, sosial, dan regional yang selaras dalam kebijakan keamanan sibernya untuk mengejar ketertinggalan dan mewujudkan kedaulatan digital.

REFERENSI

Ait Mouha, R. A. R. (2021). Internet of things (IoT). *Journal of Data Analysis and Information Processing*, *9*(77). https://doi.org/N/A

Ardiansyah & Nugroho, R. A., M. (2024). Comparative Education Policy in Cybersecurity: Lessons from East Asia. *Journal of Digital Governance*, *9*(55–68). https://doi.org/N/A

Legal, A. G. I. (2024). Cybersecurity Laws and Regulations – Indonesia. *International Comparative Legal Guide*, *N/A*(N/A). https://doi.org/N/A

UMY, A. (2024). Strengthening cybersecurity: A comparative analysis of agile policy frameworks in Southeast Asia. *N/A*, *N/A*(N/A). https://doi.org/N/A

Aspen Institute. (2024). Cybersecurity policy recommendations for the new administration. Retrieved from https://www.aspendigital.org/report/cyber-recommendations/

CISA. (2024). Cybersecurity best practices. Retrieved from https://www.cisa.gov/topics/cybersecurity-best-practices

CYFIRMA. (2025, January 31). Weekly Intelligence Report - 31 Jan 2025. Retrieved from https://www.cyfirma.com/news/weekly-intelligence-report-31-jan-2025/

Cynet. (2025). Creating your cyber security policy: Ultimate 2025 guide. Retrieved from https://www.cynet.com/cybersecurity/creating-your-cyber-security-policy-ultimate-guide/

Effendy, A. M., Sari, D. P., & Widodo, A. T. (2023). Challenges of Incident Reporting in Cybersecurity Governance in Indonesia. International Journal of Cyber Policy and Management, 18(2), 144–162.

E-Governance Academy. (2022). Indonesia – National Cyber Security Index. Retrieved from https://ncsi.ega.ee/country/id_2022/

Gunawan, R., & Lee, H. (2023). Legal Protection in Indonesia's Cyber Resilience Strategy and Implementation. Retrieved from https://www.researchgate.net/publication/388660024_Legal_Protection_in_Indonesia's_Cyber_Resilience_Strategy_and_Implementation_to_Support_National_Defense

Hasibuan, R. A. (2023). Evaluasi Efektivitas Literasi Siber pada Kurikulum Pendidikan Indonesia. Jurnal Kebijakan dan Teknologi Informasi Nasional, 11(3), 99–112.

Indosec Summit. (2024, February 13). Why cybersecurity in Indonesia needs a quick upgrade? https://www.indosecsummit.com/cybersecurity-in-indonesia-needs-quick-upgrade-most-targeted-in-region/

Infobankstore. (2023, July 15). Keamanan Siber Indonesia Peringkat Ke-5 di ASEAN, di Bawah Malaysia dan Filipina. https://infobankstore.com/artikel/1175/keamanan-siber-indonesia-peringkat-ke-5-di-asean-di-bawah-malaysia-dan-filipina

Kaspersky. (2024). Recommendations for EU cybersecurity policy for the upcoming five years. Retrieved from https://www.kaspersky.com/about/policy-blog/recommendations-for-eu-cybersecurity-policy-for-the-upcoming-five-years

KBI. (2024). 8 essential policies & procedures for improved cyber security. Retrieved from https://kbi.com.au/blog/8-essential-policies-procedures-for-improved-cyber-security/

Pemerintah Republik Indonesia. (2023). Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. https://peraturan.bpk.go.id/Details/255542/perpres-no-47-tahun-2023

Pratama, F. (2021). Urgensi Pelaporan Insiden Siber bagi Ketahanan Digital Nasional. Jurnal Keamanan Siber dan Kriptografi, 5(2), 89–103.

Putri, A. D. (2024). Indonesia's Cybersecurity Draft Law: Institutional Progress or Bureaucratic Challenge? Compliance & Risks. Retrieved from https://www.complianceandrisks.com/blog/ruu-kks-indonesias-cybersecurity-draft-law/

Rahardjo, B. (2022, November 30). Sistem Pelaporan Insiden Siber Belum Optimal, Pemerintah Perlu Buat Regulasi Khusus. Kompas.com. https://www.kompas.com/tren/read/2022/11/30/140000065/

Rahman, M. (2023). ASEAN Cyber Resilience: Indonesia’s Strategic Role. Tech for Good Institute. Retrieved from https://techforgoodinstitute.org/blog/expert-opinion/indonesias-cyber-resilience-at-the-epicenter-of-asean-digital-economy-growth/

ResearchGate. (2024). Cybersecurity index comparison with Malaysia. https://www.researchgate.net/figure/Cybersecurity-Index-Comparison-With-Malaysia_tbl4_364267812

Reuters. (2024, June 26). More than 40 Indonesian agencies hit by cyberattack on data centres. Retrieved from https://www.reuters.com/world/asia-pacific/more-than-40-indonesian-agencies-hit-by-cyberattack-data-centres-2024-06-26/

Sari, N. P. (2021, May 23). Data BPJS Kesehatan Diduga Bocor, menteri Tjahjo Dukung kemkominfo usut tuntas. Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas

Tan, Y. (2023). Cyber Governance and National Security in Southeast Asia. Lab45. Retrieved from https://www.lab45.id/detail/298/indonesia-rsquo-s-cyber-security-and-resilience-bill-strengthening-governance-or-expanding-institutional-rivalries

Widodo, D. (2020). BSSN Protects Indonesian Cyberspace. Sekretariat Kabinet Republik Indonesia. Retrieved from https://setkab.go.id/en/bssn-head-bssn-protects-indonesian-cyberspace/

Yusuf, M., & Syaifulloh, A. (2020). Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber Nasional. Jurnal Ketahanan Siber dan Sandi Negara, 2(2). Retrieved from https://scholarhub.ui.ac.id/jkskn/vol2/iss2/7/