Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial dan Politik
Volume. 2 Nomor. 3 Agustus 2025
e-ISSN: 3046-7950; p-ISSN: 3047-101X, Hal. 344-354
DOI: https://doi.org/10.62383/sosial.v2i3.2291
Tersedia: https://journal.lpkd.or.id/index.php/Sosial

Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia

Mahila Ayesha Maharani [1*], Wira Atman [2]
[1,2] Departemen Ilmu Hubungan Internasional, FISIP Universitas Hasanuddin, Indonesia
Email: mmahilaayesha@gmail.com [1], wiraatman@unhas.ac.id [2]*

Alamat: Jl. Perintis Kemerdekaan, KM 10 Kampus Universitas Hasanuddin, Tamalanrea Makassar, Indonesia 90245
** Penulis korespondensi*

Abstract. *This study aims to evaluate the effectiveness of Indonesia's National Cyber Security Strategy in responding to increasingly complex and dynamic digital threats. In the midst of the digital transformation era, Indonesia's cyberspace is vulnerable to various serious threats, such as ransomware attacks, data leaks, and the spread of disinformation that can disrupt social and political stability. This research adopts a qualitative-descriptive approach with content analysis of national strategic documents, reports from the National Cyber and Crypto Agency (BSSN), and compares them with cybersecurity policies in ASEAN countries. The results revealed that although BSSN has designed a relatively robust policy and institutional framework, its implementation is still faced with various serious obstacles, including fragmented regulations, lack of coordination between agencies, and limitations in terms of human resources. This study uses Dunn's (2023) policy evaluation framework, covering the dimensions of effectiveness, efficiency, responsiveness, equity and sustainability. The study recommends the need to strengthen governance involving various sectors, increase awareness and cyber literacy among the public, and develop national capacity through public private partnership. This evaluation is expected to serve as a basis for policy formulation to strengthen Indonesia's digital resilience, especially in the face of the increasing complexity of cyber threats at the national level.*

Keyword: *BSSN; Cybersecurity; National Strategy; Public Policy; Strategy Evaluation*

Abstrak. Penelitian ini bertujuan untuk mengevaluasi sejauh mana efektivitas Strategi Nasional Keamanan Siber Indonesia dalam merespons berbagai ancaman digital yang semakin kompleks dan dinamis. Di rengah era transformasi digital, ruang siber Indonesia berada dalam kondisi rentan terhadap berbagai ancaman serius, seperti serangan ransomware, kebocoran data, dan penyebaran disinformasi yang dapat mengganggu stabilitas sosial dan politik. Penelitian ini mengadopsi pendekatan kualitatif-deskriptif dengan analisis isi terhadap dokumen strategis nasional, laporan dari Badan Siber dan Sandi Negara (BSSN), serta membandingkannya dengan kebijakan keamanan siber di negara-negara ASEAN. Hasil penelitian mengungkapkan bahwa meskipun BSSN telah merancang kerangka kebijakan dan kelembagaan yang relatif kokoh, pelaksanaannya masih dihadapkan pada berbagai hambatan serius, antara lain regulasi yang terfregmentasi, kurangnya koordinasi antarinstansi, serta keterbatasan dalam hal sumber daya manusia. Studi ini menggunakan kerangka evaluasi kebijakan Dunn (2003), mencakup dimensi efektivitas, efisiensi, responsivitas, keadilan, dan keberlanjutan. Studi ini merekomendasikan perlunya penguatan tata kelola yang melibatkan berbagai sektor, peningkatan kesadaran dan literasi siber di kalangan masyarakat, serta pengembangan kapasitas nasional melalui kemitraan antara sektor publik swasta. Evaluasi ini diharapkan dapat menjadi landasan dalam perumusan kebijakan guna memperkuat ketahanan digital Indonesia, terutama menghadapi meningkatnya kompleksitas ancaman siber di tingkat nasional.

Kata Kunci: BSSN; Evaluasi Strategi; Keamanan Siber; Kebijakan Publik; Strategi Nasional

1. PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi (TK) telah memicu perubahan besar dalam berbagai bidang kehidupan masyarakat Indonesia. Namun, perkembangan tersebut juga membawa dampak negative berupa meningkatnya risiko dan ancaman di ranah siber, seperti peretasan, kebocoran informasi, serangan ransomware, serta penyebaran disinformasi digital. Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2023, tercatat lebih dari 300

Received: Juli 20, 2025; Revised: Agustus 13, 2025; Accepted: Agustus 29, 2025; Published: Agustus 30, 2025

juta insiden anomali lalu lintas siber, yang menuinjukkan lonjakan signifikan dibandingkan dengan tahun sebelumnya. Dalam hal ini, pemerintah Indonesia

melalui Badan Siber dan Sandi Negara (BSSN) merancang Strategi Keamanan Siber Nasional (SKSN) sebagai langkah terstruktur untuk memperkuat ketahanan nasional di bidang digital. Strategi ini ditujukan untuk membangun ruang siber yang aman, kuat, dan mendapatkan kepercayaan publik, sekaligus mendorong pembangunan nasional yang berlandaskan pada teknologi digital. Namun demikian, pelaksanaannya masih menghadapi sejumlah kendala besar, antara lain rendahnya tingkat literasi digital, tumpang tindih regulasi antar lembaga, serta keterbatasan kapasitas sumber daya manusia. Kebutuhan untuk mengevaluasi efektivitas strategi ini menjadi semakin mendesak seiring dengan meningkatnya ancaman global, seperti serangan ransomware lintas negara, aksi penyadapan data oleh aktor negara, serta maraknya hoaks yang dapat mengganggu stabilitas sosial dan politik. Dengan demikian, artikel ini bertujuan untuk melakukan evaluasi secara kritis dan menyeluruh terhadap Strategi Nasional Keamanan Siber Indonesia, dengan mengkaji arah kebijakan, implementasi program, serta pencapaian dan tantangan yang muncul dalam proses pelaksanaannya.

2. KAJIAN TEORITIS

Keamanan Siber sebagai Bagian dari Keamanan Nasional

Dengan demikian, artikel ini bertujuan untuk melakukan evaluasi secara kritis dan menyeluruh terhadap Strategi Nasional Keamanan Siber Indonesia, dengan mengkaji arah kebijakan, implementasi program, serta pencapaian dan tantangan yang muncul dalam proses pelaksanaannya. Keamanan siber saat ini merupakan elemen krusial dalam struktur pertahanan nasional setiap negara, karena mencakup aspek-aspek strategis seperti tata kelola pemerintahan digital, perlindungan data penduduk, infrastruktur vital, serta kestabilan politik dan sosial. Dunn Cavelty (2008) menyatakan bahwa keamanan siber merupakan elemen penting dalam sistem pertahanan negara, yang menuntut kemampuan negara untuk menghadapi ancaman yang bersifat asimetris, melintasi batas negara, tidak terlihat secara fisik, serta berpotensi mengganggu stabilitas sistem negara modern. Sifat serangan siber yang melampaui batas geografis dapat dilakukan oleh aktor negara maupun non-negara menjadikannya sulit untuk dideteksi dan diprediksi. Karena itu, negara dituntut tidak hanya memiliki sistem pertahanan yang kuat, tetapi juga kemampuan deteksi dini, respons cepat terhadap insiden secara real-time, serta mekanisme pemulihan *(recovery*) yang efektif dan terpercaya. Indonesia telah mulai menerapkan pendekatan ini dalam kebijakan nasional, sebagaimana tercermin dalam Peraturan

Presiden No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (IIV), yang menetapkan ruang siber sebagai salah satu objek vital nasional yang wajib dijaga dari ancaman gangguan maupun sabotase. Dokumen tersebut menegaskan peran sentral negara dalam membentuk pertahanan digital yang kuat melalui koordinasi lintas sektor, perlindungan sistemik, serta pengawasan terhadap infrastruktur vital yang dikelola baik oleh instansi pemerintah maupun pihak swasta.

Strategi Nasional dan Manajemen Risiko Siber

Secara umum, strategi keamanan siber nasional dirancang dengan mengacu pada kerangka manajemen risiko, yaitu pendekatan terstruktur untuk mengidentifikasi, meganalisis, dan mengurangi risiko yang timbul di ruang siber. Pendekatan ini menyoroti pentingnya pemahaman terhadap ancaman (threats), kelemahan sistem (vulnerabilities), serta kemungkinan dampak (impact) yang dapat ditimbulkan oleh setiap insiden yang terjadi. Organisasi seperti International Telecommunication Union (ITU) dan ASEAN telah menetapkan pedoman penyusunan strategi keamanan siber nasional. Strategi ini terdiri dari sejumlah elemen kunci, di antaranya:

Dasar hukum dan kebijakan nasional : Menjadi fondasi legal dalam menata pengelolaan siber serta menjamin perlindungan data digital. Lembaga dan sinergi antar sektor : Keberadaan institusi nasional dengan kewenangan teknis yang jelas serta sistem koordinasi antarinstansi yang terstruktur. Pelatihan dan literasi keamanan digital : Meningkatkan pemahaman serta keterampilan masyarakat dan SDM profesional dalam menghadapi tantangan dunia siber. Kerja sama internasional : peran aktif dalam forum global dan kawasan untuk mendukung kolaborasi intelijen serta peningkatan kapasitas teknologi siber. Infrastruktur nasional untuk keamanan digital : Terdiri atas mekanisme pemantauan, sistem deteksi awal, forensik siber, dan pusat komando penanganan insiden.

Melalui BSSN, Indonesia telah mengimplementasikan sebagian besar komponen dalam Strategi Nasional Keamanan Siber, yang difokuskan pada penguatan aspek teknis, pengaturan sistem elektronik, dan pengembangan tim tanggap insiden (CSIRT) lintas sektor.

Peran BSSN dalam Tata Kelola Siber Indonesia

Badan Siber dan Sandi Negara (BSSN) dibentuk sebagai lembaga nonkementerian melalui Perpres No. 53 Tahun 2017 dan disempurnakan melalui Perpres No. 133 Tahun 2017. Sebagai koordinator utama keamanan siber nasional, lembaga ini memiliki wewenang strategis dan teknis dalam merancang kebijakan, melakukan audit sistem elektronik, serta memperkuat kapasitas sumber daya manusia dan infrastruktur keamanan informasi di tingkat nasional.

Fungsi-fungsi strategis BSSN mencakup : Penyusunan dan penyelarasan regulasi teknis di bidang keamanan siber, termasuk pengembangan standar untuk sistem elektronik yang aman. Pengelolaan respons insiden siber di tingkat nasional dilakukan melalui pembentukan serta pengawasan CSIIRT di sektor publik maupun swasta. Pengembangan kapasitas dan literasi digital SDM dilakukan lewat pelatihan intensif, skema sertifikasi, serta pembentukan ekosistem pendidikan di sektor keamanan siber. Kerja sama lintas negara yang melibatkan institusi mitra internasional sepert ITU, FIRST, dan lembaga keamanan asing.

Menurut Nasution (2021), Badan Siber dan Sandi Negara (BSSN) telah menunjukkan capaian yang signifikan dalam pengembangan kerangka kerja nasional serta penguatan peran strategis senagai koordinator antar-CSIRT di tingkat nasional. Kendati demikian, sejumlah tantangan masih perlu mendapat perhatian, antara lain fragmentasi kelembagaan, rendahnya tingkat interoperabilitas sistem pelaporan insiden, serta belum optimalnya keterlibatan sektor swasta dalam mekanisme kolaborasi keamanan siber. Kurangnya sinkronisasi kebijakan antara BSSN, Kementerian Komunikasi dan Informatika, serta sejumlah lembaga sectoral lainnya masih menjadi hambatan dalam mewujudkan pelaksanaan kebijakan nasional yang konsisten dan terintegrasi.

Kerangka Evaluasi Strategi Keamanan Siber

Dalam rangka menilai efektivitas implementasi strategi nasional keamanan siber, penelitian ini mengadopsi pendekatan evaluasi kebijakan publik yang dikemukakan oleh William N. Dunn (2003). Pendekatan ini menekankan lima dimensi utama evaluasi kebijakan, yakni :

Efektivitas : Mengukur sejauh mana kebijakan yang diterapkan berhasil mencapai sasaran yang telah ditetapkan secara substantif. Efisiensi : Menilai pemanfaatan sumber daya seperti anggaran, waktu, dan tenaga kerja secara optimal dalam proses implementasi kebijakan. Responsivitas : Mencermikan kemampuan kebijakan untuk merespons kebutuhan nyata masyarakat dan pelaku usaha secara tepat waktu dan relevan. Keadilan : Menunjukkan tingkat inkluvsivitas kebijakan terhadap berbagai kelompok masyarakat, khususnya kelompok rentan dan daerah tertinggal, dalam proses maupun hasil kebijakan. Keberlanjutan : Menggambarkan ketahanan kebijakan terhadap perubahan jangka panjang, termasuk pergeseran pemerintahan serta perkembangan teknologi dan lingkungan strategis.

Pendekatan evaluatif ini memberikan ruang bagi peneliti untuk melampaui penilaian berbasis output administrative (seperti sejumlah CSIRT yang telah dibentuk), dengan turut memperhatikan dampak substansif dari strategi terhadap penguatan ketahanan nasional, perlindungan data pribadi warga negara, serta peningkatan kapasitas mitigasi risiko siber

secara komprehensif. Evaluasi yang mengacu pada dimensi-dimensi tersebut menjadi krusial untuk menjamin bahwa strategi yang disusun tidak semata bersifat normatif, melainkan juga mampu bersifat adaptif terhadap dinamika ancaman, mendorong partisipasi aktif para pemangku kepentingan, serta berfokus pada pencapaian hasil yang terukur dan berdampak.

3. METODE PENELITIAN

Untuk memahami implementasi Strategi Nasional Keamana Siber di Indonesia, penelitian ini menggunakan metode deskriptif kualitatif. Data yang digunakan berasal dari dokumen sekunder seperti peraturan presiden, strategi resmi BSSN, laporan tahunan BSSN (2019-2023) serta indeks dan laporan dari lembaga internasional seperti ASEAN dan ITU. Analisis literatur dari jurnal ilmiah juga digunakan. Metode analisis isi digunakan untuk melakukan analisis. Ini melibatkan membandingkan strategi BSSN dengan standar internasional seperti *Global Cybersecurity Index* dan mengaitkannya dengan lima dimensi evaluasi kebijakan menurut Dunn: keberlanjutan, keadilan, efektivitas, responsivitas, dan efisiensi. Dengan triangulasi sumber dan analisis tren dari waktu ke waktu, validitas data diperkuat. Penelitian ini tidak menggunakan data primer seperti wawancara, namun tetap mampu menyusun evaluasi yang menyeluruh berkat pemanfaatan sumber-sumber resmi dan literatur akademik yang terpercaya.

4. HASIL DAN PEMBAHASAN

Strategi Nasional Keamanan Siber Indonesia

Indonesia telah menyusun Strategi Nasional Keamanan Siber sebagai langkah strategis dan terstruktur untuk merespons eskalasi ancaman digital yang kian kompleks dan berkembang. Strategi ini dituangkan dalam berbagai kebijakan utama seperti Peraturan Presiden No. 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN), serta sejumlah regulasi turunannya. Strategi tersebut dibangun diatas lima pilar utama, yakni tata kelola yang efektif, pengelolaan risiko siber, mekanisme respons insiden yang terintegrasi, penguatan kapasitas sumber daya manusia, serta kerja sama internasional dalam menghadapi ancaman global. Dalam ranah tata kelola, BSSN berperan sebagai otoritas utama dalam merumuskan regulasi teknis yang mencakup pengelolaan sistem elektronik, perlindungan kerahasiaan data, serta prosedur mitigasi terhadap insiden siber. Namun demikian, implementasi pilar manajemen risiko masih menghadapi keterbatasan dalam menjangkau sektor non-pemerintah, terutama usaha mikro, kecil, dan menengah (UMKM) serta institusi pendidikan, yang umumnya rentan terhadap serangan siber akibat lemahnya sistem perlindungan internal dan

keterbatasan sumber daya yang dimiliki. (Wahyudi, R, 2020)

Evaluasi Implementasi oleh BSSN

Sejak 2018, BSSN telah mencatat sejumlah capaian strategis, antara lain: Pembentukan lebih dari 120 Tim Tanggap Insiden Keamanan Siber (CSIRT) di berbagai lembaga dan institusi. Pengintegrasian sistem pelaporan insiden siber pada tingkat nasional. Pelaksanaan program pelatihan sumber daya manusia melalui inisiatif Digital Talent Scholarship. Peningkatan kesadaran publik terhadap isu keamanan digital melalui program literasi digital massal yang dilaksanakan bersama Kementerian Komunikasi dan Informatika.

Namun, kondisi di tingkat implementasi menunjukka bahwa sejumlah CSIRT di daerah masih menghadapi keterbatasan kapasitas teknis, serta belum tersedianya mekanisme interoperabilitas yang standar antar-CSIRT di berbagai wilayah dan sektor. Keterbatasan tersebut berdampak pada lambatnya respons terhadap insiden siber dan menimbulkan ketidakjelasan dalam prosedur pelaporan serta mekanisme eskalasi masalah. (BSSN,2023) Hasil evaluasi turut mengindikasikan adanya kesenjangan signifikan antara institusi pusat dan daerah dalam pelaksanaan audit keamanan siber. Pelaksanaan fungsi audit oleh BSSN masih belum berlangsung secara optimal dan menyeluruh di seluruh instansi. Padahal, audit berkala ini merupakan komponen krusial dalam upaya peningkatan mutu pengamanan sistem elektronik nasional. (Yuliana & Nugraha 2022)

Ancaman Siber Indonesia Saat Ini

Ancaman di ruang siber yang dihadapi Indonesia tidak semata-mata bersifat teknis, melainkan juga mengandung dimensi sosial-politik. Mengacu pada laporan BSSN serta Global Threat Landscape ENISA (2023), beberapa bentuk ancaman yang paling menonjol di Indonesia meliputi:

Ransomware dan malware: Menjadi ancaman utama yang menyasar institusi strategis seperti rumah sakit, perguruan tinggi, dan instansi pemerintahan. Salah satu insiden signifikan terjadi pada tahun 2022, Ketika sebuah universitas negeri ternama mengalami serangan ransomware yang mengakibatkan kerugian finansial mencapai lebih dari Rp1,5 miliar. Phising dan social engineering: Merupakan ancaman yang banyak ditujukan kepada pengguna platform e-commerce, perbankan, serta aplikasi dompet digital. Hasil survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa sekitar 47% responden pernah menerima email atau tautan mencurigakan yang diduga merupakan upaya pencurian data pribadi. Disinformasi dan konten manipulatif: Intensitas penyebaran informasi palsu mengalami peningkatan signifikan menjelang momentum politik, seperti Pemilu 2024. Pemanfaatan algoritma media sosial dalam distribusi hoaks berisiko menciptakan polarisasi

sosial dan mengganggu kohesi masyarakat. Kebocoran data pribadi: sejumlah insiden berskala besar, seperti kebocoran data yang menimpa KPU, PLN, dan BPJS Kesehatan, telah memberikan dampak negatif terhadap citra keamanan digital nasional. Kejadian-kejadian ini mencerminkan lemahnya infrastruktur dan mekanisme perlindungan data pada institusi-institusi strategis negara.

Perbandingan Strategi Keamanan Siber Indonesia dengan Negara Lain

Guna memperoleh pemahaman yang lebih holistic mengenai efektivitas Strategi Nasional Keamanan Siber Indonesia, diperlukan analisis komparatif dengan sejumlah negara yang dinilai berhasil dalam membangun sistem keamanan siber yang tangguh dan terintegrasi. Sebagai contoh, Singapura menerapkan pendekatan strategis yang terstruktur melalui *National Cybersecurity Blueprint* yang dikelola secara terpusat oleh *Cyber Security Agency of Singapore* (CSA). Negara ini memiliki sejumlah inisiatif kunci seperti National *Cybersecurity Masterplan*, *Crticial Information Infrastructure Protection Programme*, serta laporan tahunan *Singapore Cyber Landscape Report* yang digunakan untuk mengevaluasi capaian dan tantangan keamanan siber secara berkelanjutan. Salah satu aspek menonjol dari strategi Singapura adalah penerapan standar keamanan siber yang bersifat wajib bagi sektor-sektor kritis seperti energi, kesehatan, dan keuangan. (CSA Singapore, 2022)

Di sisi lain, Malaysia telah mengembangkan kerangka hukum yang kokoh melalui *Malaysia Cybersecurity Strategy 2020-2024*, yang dirancang untuk mendukung lima tujuan nasional utama, termasuk penguatan infrastruktur teknis dan pengembangan ekosistem kolaboratif dalam keamanan siber. Implementasi strategi ini dijalankan oleh lembaga pelaksanaan teknis, *Cybersecurity Malaysia*, yang beroperasi di bawah naungan Kementerian Komunikasi dan Multimedia, berperan sebagai otoritas utama dalam pengembangan kapasitas, mitigasi insiden, serta edukasi publik terkait ancaman siber.

Jika dibandingkan dengan negara-negara seperti Singapura dan Malaysia, Indonesia masih menghadapi sejumlah kesenjangan strategis yang signifikan dalam pengelolaan keamanan siber nasional. Pertama, belum tersedia strategi formal jangka panjang yang disertai dengan mekanisme evaluasi berkala serta pembaruan indikator kinerja secara sistematis. Kedua, penegakan hukum terhadap insiden kebocoran data masih lemah, baik dari segi pemberian sanksi maupun efektivitas mekanisme pelaporan dan investigasi. Ketiga, pendekatan berbasis manajemen risiko pada sektor-sektor kritikal seperti energi, transportasi, dan layanan publik masih minim, sehingga menimbulkan kerentanan sistematik terhadap potensi gangguan digital. Oleh karena itu, dapat disimpulkan bahwa Indonesia masih membutuhkan upaya intensif dalam mengintegrasikan kebijakan keamanan siber secara

menyeluruh, menyusun peta jalan strategis jangka panjang yang adaptif terhadap dinamika ancaman digital, serta memperkuat kapasitas kelembagaan pelaksanaan dengan mandat teknis yang jelas dan kewenangan koordinatif lintas sektor.

Urgensi Penerapan Pendekatan Ketahanan Siber (*Cyber Resilience*)

Sebagian besar kebijakan strategis keamanan siber nasional masih terpusat pada pendekatan preventif dan mitigatif dalam menghadapi potensi ancaman digital. Akan tetapi, dengan semakin kompleks dan tak terduganya pola serangan siber, menjadikan krusial bagi Indonesia untuk mulai mengimplementasikan pendekatan ketahanan siber (cyber resilience). Konsep ketahanan siber tidak semata-mata berfokus pada perlindungan teknis, melainkan juga mencakup kemampuan untuk mendeteksi anomali secara dini, merespons secara adaptif dan otomatis, memulihkan layanan esensial dengan waktu henti yang minimal, serta membangun sistem yang dapat belajar dari setiap insiden guna memperkuat mekanisme perlindungan di masa mendatang. Pendekatan ini menuntut pembaruan yang berkelanjutan terhadap prosedur operasional dan perangkat teknologi, serta partisipasi aktif dari seluruh pemangku kepentingan, termasuk kalangan masyarakat sipil. Pelaksanaan *cyber drills*, simulasi insiden berskala nasional, serta audit terhadap ketahanan sistem perlu diprioritaskan sebagai bagian integral dari roadmap keamanan siber Indonesia.

Peran Masyarakat dan Sektor Swasta dalam Ketahanan Siber

Strategi nasional yang semata-mata mengandalkan peran institusi pemerintah tidak memadai untuk merespons ancaman digital yang bersifat multidomain dan lintas sektor. Peran masyarakat dan sektor swasta menjadi elemen krusial dalam membangun serta memperkuat ekosistem keamanan siber yang berkelanjutan. Sayangnya, tingkat partisipasi sektor swasta dalam mekanisme pelaporan insiden siber masih tergolong rendah. Banyak entitas perusahaan enggan menyampaikan laporan insiden karena kekhawatiran akan dampak negatif terhadap reputasi, serta ketiadaan regulasi yang secara tegas mewajibkan pelaporan tersebut. Di samping itu, implementasi inisiatif Tanggung Jawab Sosial Perusahaan (CSR) yang berfokus pada peningkatan literasi siber masih sangat minim dan belum menjadi prioritas utama bagi sebagian besar pelaku usaha.

Rekomendasi Kebijakan

Berdasarkan temuan dalam penelitian ini, sejumlah rekomendasi kebijakan dapat diajukan sebagai upaya memperkuat strategi keamanan siber nasional Indonesia: Penguatan tata kelola lintas sektor, melalui pembentukan mekanisme koordinasi yang bersifat regular dan terstruktur antara BSSN, Kementerian Komunikasi dan Informatika, Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan, serta pemangku kepentingan strategis lainnya.

Perumusan peta jalan (roadmap), keamanan siber nasional yang lebih terarah, dengan penetapan sasaran jangka pendek, menengah, dan panjang, disertai indikator kinerja yang jelas untuk mengukur kemajuan secara berkala. Reformulasi kerangka regulasi, dengan mendorong percepatan pengesahan dan penerapan Undang-Undang Perlindungan Data Pribadi, serta integrasi substansinya,ke dalam sistem pengawasan dan penegakan hukum yang dijalankan oleh BSSN. Peningkatan investasi berkelanjutan dalam pengembangan kapasitas SDM di bidang keamanan siber, melalui penyediaan intensif pendidikan, program pelatihan dan sertifikasi nasional, serta pendirian pusat keunggulan (*center of excellence*) di berbagai wilayah strategis. Peningkatan partisipasi sektor swasta dan masyarakat sipil, termasuk penerapan regulasi *mandatory disclosure* untuk insiden siber, serta pemberian intensif bagi pelaporan insiden dan keterbukaan informasi kepada publik. Penguatan kerja sama internasional, baik dalam kerangka bilateral maupun multilateral, mencakup kolaborasi dalam deteksi dini ancaman, pertukaran intelijen siber, pelaksanaan simulasi krisis, dan pengembangan teknologi perlindungan digital nasional.

5. KESIMPULAN

Studi ini menekenankan urgensi dilakukannya evaluasi komprehensif terhadap Strategi Nasional Keamanan Siber Indonesia guna merespons dinamika ancaman digital yang kian kompleks dan berkembang pesat. Hal analisis terhadap dokumen strategis, laporan tahunan BSSN, serta perbandingan dengan negara-negara ASEAN menunjukkan bahwa Indonesia telah membangun landasan kebijakan yang relatif solid, namun masih dihadapkan pada sejumlah tantangan krusial terkait pelaksanaan kebijakan dan peningkatan kapabilitas teknis di lapangan. Dari perspektif kelembagaan, pendirian Badan Siber dan Sandi Negara (BSSN) merupakan langkah strategis yang bertujuan untuk mengonsolidasikan komando serta menyelaraskan arah kebijakan nasional di bidang keamanan siber. Namun, dalam implementasinya, efektivitas BSSN masih terhambat oleh lemahnya koordinasi lintas kementerian, ketimpangan dalam alokasi anggaran, serta lambannya pengembangan infrastruktur forensik digital yang memadai.

Di lain pihak, inisiatif pembentukan tim CSIRT serta pelaksanaan kampanye literasi digital telah memberikan dampak positif, meskipun penyebarannya masih belum merata baik dari segi wilayah geografis maupun sektor terkait. Beragam ancaman digital, seperti serangan ransomware, kebocoran data pribadi, gangguan terhadap infrastruktur kritikal, serta penyebaran disinformasi sepanjang Pemilu, mengindikasikan bahwa pendekatan strategis yang statis dan reaktif tidak lagi memadai dalam menghadapi dinamika lanskap siber saat ini. Dengan demikian, diperlukan adopsi pendekatan baru yang berlandaskan pada prinsip

ketahanan siber (cyber resilience), yang mengutamakan kemampuan adaptif, respons cepat terhadap insiden, pemulihan sistem secara efisien, serta pembelajaran berkelanjutan dari setiap gangguan yang terjadi. Hasil perbandingan dengan praktik di Singapura dan Malaysia menggarisbawahi perlunya percepatan adopsi strategi jangka panjang di Indonesia yang didasarkan pada indikator kinerja yang terukur, penguatan kapasitas lembaga teknis pelaksana, serta perumusan tata kelola yang bersifat transparan dan melibatkan partisipasi berbagai pemangku kepentingan. Salah satu kelemahan paling signifikan terletak pada belum optimalnya integrasi antara strategi keamanan siber nasional dan agenda transformasi. Melalui pengaturan strategi keamanan siber nasional yang bersifat inklusif, terintegratif, dan berorientasi pada prinsip ketahanan (*resilience*), Indonesia memiliki peluang untuk menghadapi tantangan digital kontemporer dan yang akan datang dengan lebih solid, sekaligus menjaga kedaulatan digital serta melindungi kepentingan nasional di tengah dinamika globalisasi teknologi yang terus berkembang.

DAFTAR PUSTAKA

ASEAN Secretariat. (2021). *ASEAN Cybersecurity Cooperation Strategy 2021-2025*. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Bayuk, J. L., Horowitz, B., et al. (2012). *Cybersecurity Policy Guidebook*. Wiley. https://cerutties.wordpress.com/wp-content/uploads/2015/09/cyber-security-policy-guidebook.pdf

BSSN. (2022). *Laporan Tahunan Badan Siber dan Sandi Negara*. Jakarta: BSSN. https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

BSSN. (2023). Statistik insiden siber Indonesia tahun 2023. Diakses dari https://bssn.go.id/statistik2023

Dunn, W. N. (2003). *Pengantar analisis kebijakan publik*. Yogyakarta: Gadjah Mada University Press. https://ugmpress.ugm.ac.id/en/product/ekonomi-bisnis/pengantar-analisis-kebijakan-publik

ITU. (2022). *Global Cybersecurity Index*. Diakses dari https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

Kominfo. (2022). *Roadmap transformasi digital Indonesia*. https://www.komdigi.go.id/berita/artikel/detail/peta-jalan-mempercepat-transformasi-digital

Kurniawan, A. (2023). Perbandingan strategi keamanan siber ASEAN. *Jurnal Keamanan Regional, 3*(1), 12-25.

Lewis, J. A. (2014). *Cybersecurity and Cyberwarfare: Assessing U.S. Policy*. CSIS Press. https://scholar.google.co.id/scholar?q=Lewis,+J.+A.+(2014).+Cybersecurity+and+Cyberwarfare:+Assessing+U.S.+Policy.+CSIS+Press&hl=id&as_sdt=0&as_vis=1&oi=scholart

Nurcahyo, D. (2022). Resilensi digital dalam perspektif nasional. *Jurnal Ilmu Kebijakan Publik, 8*(2), 45-58.

OECD. (2020). *Digital Security Policy Framework*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/oecd-policy-framework-on-digital-security_a0b1d79c/a69df866-en.pdf

Peraturan Presiden No. 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN).

Wahyudi, R. (2020). Kebijakan perlindungan data pribadi di Indonesia. *Jurnal Hukum dan Teknologi, 5*(3), 99-112.

Wicaksono, R. (2021). Analisis kesiapan implementasi strategi keamanan siber nasional. *Jurnal Keamanan Informasi, 6*(2), 88-101.

Yuliana, T., & Nugraha, F. (2022). Kebijakan transformasi digital dan tantangannya dalam keamanan siber. *Jurnal Kebijakan Digital, 4*(1), 23-36.