Madani: Jurnal Ilmiah Multidisiplin
Volume 4, Nomor 5, June 2026, P. 200-206
E-ISSN: 2986-6340
Licenced by CC BY-SA 4.0
DOI: https://doi.org/10.5281/zenodo.20775741

Ancaman Siber terhadap Infrastruktur Kritis Indonesia: Analisis Kebijakan Keamanan Nasional di Era Digital

Jihan Aqilah Idris Sadik
Universitas Hasanuddin, Makassar

Abstrak

Seiring dengan pesatnya perkembangan era digital, infrastruktur kritis di Indonesia, khususnya pada sektor energi, telekomunikasi, dan keuangan, semakin rentan terhadap berbagai serangan siber. Beragam ancaman, seperti ransomware, serangan Distributed Denial of Service (DDoS), serta spionase siber yang didukung oleh negara tertentu, terus mengalami peningkatan. Penelitian ini bertujuan untuk mengkaji efektivitas kebijakan keamanan nasional Indonesia, khususnya Peraturan Pemerintah Nomor 42 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Metode penelitian yang digunakan adalah metode kualitatif melalui analisis dokumen kebijakan serta studi kasus serangan siber berskala besar, seperti serangan WannaCry pada tahun 2017 dan serangan terhadap PLN pada tahun 2022. Hasil penelitian menunjukkan bahwa kebijakan yang ada saat ini masih menghadapi berbagai tantangan, antara lain lemahnya koordinasi antarlembaga, keterbatasan sumber daya manusia di bidang keamanan siber, serta belum optimalnya pemanfaatan teknologi kecerdasan buatan (Artificial Intelligence atau AI) untuk deteksi ancaman secara dini. Oleh karena itu, diperlukan reformasi kebijakan yang lebih berorientasi pada pendekatan berbasis risiko, penguatan kerja sama antara pemerintah dan sektor swasta, serta peningkatan kesadaran masyarakat mengenai keamanan siber.

Kata kunci: *ancaman siber, infrastruktur kritis, kebijakan keamanan nasional, Indonesia, era digital.*

Abstract

As the digital era continues to advance rapidly, critical infrastructure in Indonesia, particularly in the energy, telecommunications, and financial sectors, has become increasingly vulnerable to cyberattacks. Various cyber threats, including ransomware, Distributed Denial of Service (DDoS) attacks, and state-sponsored cyber espionage, are growing in frequency and sophistication. This study aims to examine the effectiveness of Indonesia's national cybersecurity policies, specifically Government Regulation No. 42 of 2023 concerning the National Cybersecurity Strategy and Law No. 11 of 2008 concerning Electronic Information and Transactions. The research employs a qualitative approach through policy document analysis and case studies of major cyberattacks, including the WannaCry attack in 2017 and the attack on PLN in 2022. The findings indicate that existing policies continue to face several challenges, such as weak inter-agency coordination, a shortage of cybersecurity professionals, and the suboptimal utilization of Artificial Intelligence (AI) technologies for early threat detection. Therefore, policy reforms are needed to emphasize a risk-based approach, strengthen public-private partnerships, and enhance public awareness of cybersecurity issues.

Keywords: *cyber threats, critical infrastructure, national cybersecurity policy, Indonesia, digital era.*

PENDAHULUAN

Transformasi digital besar-besaran di Indonesia menghasilkan situasi peluang dan risiko yang belum pernah terjadi sebelumnya, yang digambarkan sebagai dua sisi mata uang yang sama. Dengan proyeksi penetrasi internet lebih dari 215 juta pengguna pada tahun 2024, pertumbuhan ekonomi digital, dan digitalisasi layanan publik melalui Sistem Pemerintahan Berbasis Elektronik (SPBE), infrastruktur digital Indonesia merupakan aset strategis nasional dan target potensional bagi pelaku ancaman siber. Dalam konteks ini, infrastruktur kritis atau Infrastruktur Informasi Vital (IIV) adalah infrastruktur yang jika terganggu atau hancur, akan berdampak buruk atau kemungkinan besar akan berdampak buruk pada keamanan nasional, keamanan ekonomi nasional, kesehatan atau keselamatan publik, atau kombinasi dari hal-hal tersebut (peraturan presiden no. 82 tahun 2022). Sektor-sektor yang termasuk dalam kategori IIV di Indonesia adalah energi (listrik, minyak, dan gas), air, transportasi, keuangan dan perbankan, kesehatan dan teknologi informasi pemerintah.

Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan peningkatan ancaman yang mengkhawatirkan. Pada tahun 2021, Indonesia mencatat lebih dari 1,6 miliar serangan siber. Tahun 2022 menyaksikan lonjakan sebesar 38% dalam serangan *ransomware Brain Cipher* berbasis *LockBit* 3.0 melumpuhkan Pusat Data Nasional Sementara (PDNS) dan mengganggu 282 layanan publik dengan tuntutan tebusan sebesar 8 juta dollar AS, menjadikannya krisis keamanan siber terbesar dalam sejarah transformasi digital pemerintah Indonesia. Pertanyaan utama dari penelitian ini adalah seberapa memadai kebijakan keamanan nasional Indonesia dalam menghadapi ancaman dunia terhadap infrastruktur nasional yang kritis?Dan kesenjangan struktural apa yang perlu segera diisi?. Penelitian ini bertujuan untuk memetakan typologi dan tren ancaman siber terhadap IIV Indonesia, mengevaluasi kerangka kebijakan keamanan siber yang ada, dan merumuskan rekomendasi kebijakan berbasis bukti untuk memperkuat ketahanan siber nasional.

TINJAUAN PUSTAKA

Konsep Keamanan Siber dan Infrastruktur Kritis

Dalam pembicaraan akademis dimasa sekarang ini, keamanan siber tidak lagi dipandang sebagai upaya teknis hanya untuk melindungi sistem komputer. Bidang ini sudah berubah menjadi bagian integral dari keamanan nasional beberapa pakar bahkan menyebutnya sebagai wilayah kelima disepanjang daratan, laut, udara, dan luar angkasa. Sifat ancaman siber terhadap infrastruktur kritis adalah asimetris, aktor non-negara, kelompol kriminal terorganisir, dan bahkan individu tunggal memiliki kemampuan untuk melumpuhkan layanan publik berskala nasional. Penelitian oleh Cloramidine dan Badaruddi (2023) atas keamanan internet Indonesia yang berdiri di indeks keamanan siber global (GCI) menunjukkan bahwa Indonesia tetap berada dalam kategori negara yang membutuhkan perbaikan besar, khususnya dalam bidang perundang-undangan, kapasitas teknis, dan kerjasama internasional. Penelitian ini menunjukkan bahwa memiliki peraturan saja tidak memadai untuk diterapkan dan kapasitas kelembagaan yang kuat adalah penentu keberhasilan. [1]

[1] Feline Cloramidine and Muhammad Badaruddin, "MENGUKUR KEAMANAN SIBER INDONESIA MELALUI INDIKATOR PILAR KERJASAMA DALAM GLOBAL CYBERSECURITY INDEX (GCI)" 8 (2023): 57–73.

Kerangka Hukum dan Kebijakan Siber Indonesia

Dalam hal tata kelola keamanan siber, Indonesia memiliki beberapa instrumen hukum yang relevan. Undang-Undang No. 11 Tahun 2008 mengenai Informasi dan Transaksi Ekonomi (ITE) yang di update melalui Undang-Undang No. 19 Tahun 2016 adalah dasar hukum awal. Kemudian ada Peraturan Presiden (Perpres) No. 53 tahun 2017 dalam menetapkan BSSN sebagai otoritas keamanan siber nasional yang memperkuat struktur kelembagaan. Momentum regulasi yang terbaru hadir dalam Undang-Undang No. 27 Tahun 2022 mengenai perlindungan data pribadi dan peraturan presiden, No. 82 Tahun 2022 tentang perlindungan Infrastruktur Informasi Vital.[2] Namun demikian, Bua dan Idris (2025) dalam analisis kebijakan mereka atas kebocoran data nasional 2024 menemukan bahwa peraturan yang ada masih menghadapi isu-isu implementasi yang serius, pembagian otoritas di antara kementrian, kurangnya mandatori pelaporan insiden, dan belum ada standar keamanan yang mengikat Infrastruktur Informasi Vital.[3]

Tren Ancaman Siber Global dan Regional

Dalam konteks global, Watney (2022) meneliti ancaman siber terhadap infrastruktur kritis dari sudut pandang hukum dan menyimpulkan bahwa atribusi serangan siber yang sulit, serta ketidakjelasan norma-norma internasional dalam hukum siber, menciptakan zona abu-abu yang dimanfaatkan oleh para pelaku ancaman.[4] Sementara itu, laporan CrowdStrike (2024) untuk wilayah Asia pasifik menunjukkan peningkatan aktivitas APT yang disponsori negara, dengan sektor energi dan keuangan sebagai target utama. Pada tingkat regional, dikajian Cordes et al dalam *Journal of Information Policy* mengungkapkan bahwa negara-negara ASEAN, termasuk Indonesia sudah menjadi salah satu target insiden siber tertinggi di Asia Tenggara antara tahun 2020-2023, dengan kerentanan sistematik berupa regulasi yang tidak memadai dan rendahnya kapasitas respons insiden.[5]

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode analisis kebiajakan. Pengumpulan data dengan melalui dua jalur utama. Pertama, studi dokumen meliputi peraturan dan kebijakan resmi pemerintah Indonesia (UU, peraturan presiden, peraturan BSSN), laporan tahunan BSSN (2021-2024), laporan insiden dari ID-SIRTII/CC termasuk dokumen internasional seperti ITU *Global Cybersecurity Index* dan laporan ASEAN-SIRT. Kedua, tinjauan literatur yang sistematis tentang artikel jurnal ilmiah, proses konferensi, dan laporan tentang lembaga terpercaya yang berkaitan dengan keamanan siber, baik nasional maupun internasional. Analisis kebijakan dilakukan melalui kerangka evaluasi lima dimensi William N. Dunn (2023), efektivitas, efesiensi, kecukupan, kesetaraan, dan responsif kebijakan.[6] Studi kasus insiden pada bulan juni 2024 PDNS digunakan sebagai instrumen triangulasi untuk mengukuhkan temuan analisis kebijakan.

[2] Bupati Konawe et al., "No Title," 2021.

[3] Imanuel Toding Bua and Nur Isdah Idris, "Analisis Kebijakan Keamanan Siber Di Indonesia : Studi Kasus Kebocoran Data Nasional Pada Tahun 2024" 2 (2025): 100–114.

[4] Murdoch Watney, "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure : A Legal Perspective," 2021, 319–27.

[5] Monica Nila Sari, "Cybercrime in Association of Southeast Asian Nations Regional Effort and Its Effectiveness" 14 (n.d.).

[6] *Public Policy Analysis Dunn*, n.d.

Penelitian mencakup periode waktu 2020-2024 dan difokuskan pada kebijakan keamanan siber nasional dan pengaruhnya pada sektor Infrastruktur Informasi Vital.

HASIL

Lanskap Ancaman Siber terhadap Infrastruktur Kritis Indonesia

Data dari BSSN dan berbagai sumber lain, ancaman siber terhadap infrastruktur vital Indonesia sebenarnya bisa dikelompokkan ke dalam lima jenis utama dan semuanya menunjukkan tren yang semakin mengkhawatirkan, baik dari segi frekuensi maupun tingkat kerumitannya. Yang pertama dan paling merusak adalah ransomware. Dua peristiwa besar yang sulit dilupakan adalah serangan LockBit ke Bank Syariah Indonesia (BSI) pada Mei 2023, yang berhasil mencuri sekitar 1,5 terabyte data nasabah dan serangan Brain Cipher LockBit 3.0 yang melumpuhkan PDNS pada Juni 2024.[7] Sepanjang 2023, BSSN mencatat lebih dari 1 juta aktivitas ransomware. Survei Fortinrt-IDC bahkan menunjukkan bahwa lebih dari 60% perusahaan Indonesia mengaku mengalami lonjakan serangan jenis ini, jumlahnya dua kali lipat dibanding tahun sebelumnya.[8]

Kedua adalah APT atau *Advance Persistent Threat.* Ini merupakan ancaman yang lebih serius dari sisi strategi karena pelakunya terorganisir, tidak terburu-buru, dan seringkali mendapat dukungan dari negara atau kepentingan geopolitik tertentu.[9] BSSN mencatat hampir 4 juta aktivitas APT selama 2023, meningkat cukup tajam. Pada 2022, dari total 84,8 juta serangan siber yang terjadi di Indonesia, sekitar 1,7 juta diantaranya secara spesifik mengincar sektor pertahanan.[10] Ketiga, serangan DDoS masih sering dipakai untuk melumpuhkan layanan publik digital. Keempat, phishing dan rekayasa sosial tetap menjadi pintu masuk yang paling umum digunakan penyerang lebih dari 50 ribu laporan masuk pada tahun 2023. Dan kelima, perusakan situs web pemerintah terus terjadi, biasanya sebagai bentuk pesan politis atau ekspresi aktivisme di dunia digital.

Studi Kasus: Serangan PDNS 2024 sebagai Cermin Kerentanan Sistematik

Insiden yang menimpa Pusat Data Nasional Sementara (PDNS) 2 di Surabaya pada 20 Juni 2024 penting untuk dikaji lebih dalam, bukan semata karena dampaknya yang besar, tapi karena memperlihatkan kelemahan yang sudah mengakar, bukan sekedar kecelakaan teknis yang kebetulan terjadi. Kronologisnya, tanda-tanda serangan sudah mencul sejak 17 Juni, ketika ada uapaya mematikan Windows Defender. Tiga hari kemudian, ransomware Brain Cipher berhasil mengenkripsi data dan melumpuhkan sistem. Akibatnyaa, 282 layanan publik terganggu sekaligus, mulai dari sistem imigrasi di Bandara Soekarno-Hatta, layanan beasiswa KIP, hingga berbagai portal kementrian. Para penyerang meminta tebusan $8 juta atau sekitar Rp131 miliar, lalu secara mengejutkan beberapa minggu kemudian menyatakan akan memberikan kunci dekripsi secara gratis, seuatu yang jarang sekali terjadi dalam kasus ransomware. Setelah insiden diselidiki, ditemukan sejumlah akar masalah yaitu, tidak ada sistem backup yang memadai dan terpisah, perangkat lunak yang dibiarkan kadaluwarsa tanpa pembaruan, konfigurasi keamanan yang longgar, protokol respons insiden yang belum pernah benar-benar diuji, dan

[7] Bua and Idris, "Analisis Kebijakan Keamanan Siber Di Indonesia : Studi Kasus Kebocoran Data Nasional Pada Tahun 2024."

[8] "LKJ-BSSN-2023_Sign.Pdf," n.d.

[9] Watney, "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure : A Legal Perspective."

[10] "LKJ-BSSN-2023_Sign.Pdf."

yang tidak kalah penting adalah kewenangan yang terfragmentasi antara BSSN dan Kemenkominfo sehingga respons pun menjadi lambat.[11]

Evaluasi Kebijakan Keamanan Siber Nasional

Menggunakan kerangka analisis Dunn (2003), kebijakan keamanan siber Indonesia menghasilkan gambaran yang cukup beragam.[12] Dari sisi efektivitas, regulasi yang ada terutama Perpres No. 82 Tahun 2022 sebetulnya sudah cukup lengkap secara normatif dalam mengatur perlindungan infrastruktur vital.[13] Masalahnya, insiden PDNS membuktikan bahwa aturan di atas kertas belum benar-benar dijalankan di lapangan. Survei 2024 menunjukkan hanya 12% organisasi Indonesia yang kematangan keamanan sibernya bisa dibilang memadai, sementara hampir sebagiannya yang masih berada di tahap paling awal.

Dari sisi kelembagaan, BSSN memang sudah ada sebagai otoritas siber nasional, tapi kapasitasnya masih jauh dari ideal. Anggarannya tidak sebanding dengan ancaman yang dihadapi, kewenangannya masih tumpang tindih dengan Kominfo, BIN, dan lembaga lain, dan sumber daya manusianya dengan keahlian siber tingkat lanjut masih sangat terbatas. Koordinasi lintas lembaga tetap menjadi titik lemah yang paling menonjol. Dari sisi legislasi, kehadiran UU PDP No. 27 Tahun 2022 patut diapresiasi sebagai langkah maju. Namun belum ada pedoman teknis yang cukup rinci soal kewajiban pelaporan insiden bagi pengelola infrastruktur kritis, dan mekanisme sanksinya pun masih belum terlau jelas. Harminisasi antara UU ITE, UU PDP, dan regulasi sektoral juga masih menjadi pekerjaan rumah yang belum tuntas.

Perbandingan dengan Kerangka Internasional

Dibanding standar Internasional, Indonesia masih punya jarak yang cukup jauh untuk dikejar. NIST *Cybersecurity Framework* mengenal lima fungsi inti yaitu, *identify, protect, detect, respond,* dan *recover.* Insiden PDNS menunjukkan kelemahan di seluruh fungsi itu dari pencatatan aset yang tidak tuntas hingga pemulihan yang memakan waktu terlalu lama.[14] Di ASEAN sendiri, Singapura sudah selangkah lebih jauh dengan mendirikan *Digital and Intelligence Service* (DIS) pada 2022, yang secara resmi mengintegrasikan pertahanan siber ke dalam struktur pertahanan nasional. Indonesia sedang berupaya menempuh jalan serupa melalui TNI *Cyberforce* yang dibentuk pada 2023, meski prosesnya masih berjalan. Dari kajian komparatif terhadap negara-negara dengan ketahanan siber tinggi, ada empat kesamaan yang mencolok, mereka mewajibkan standar keamanan untuk infrastruktur kritis, punya otoritas siber tunggal dengan mandat yang kuat, memiliki mekanisme berbagai informasi publik-swaste yang jelas, dan mengalokasikan anggaran pertahanan siber secara proporsional. Indonesia, saat ini belum memenuhi semua kriteria tersebut secara konsisten.[15]

[11] Bua and Idris, "Analisis Kebijakan Keamanan Siber Di Indonesia : Studi Kasus Kebocoran Data Nasional Pada Tahun 2024."

[12] Fifth Edition, "Fifth Edition," n.d.

[13] Konawe et al., "No Title."

[14] "Framework for Improving Critical Infrastructure Cybersecurity," 2018.

[15] Leandros Maglaras and Helge Janicke, "Cybersecurity of Critical Infrastructures : Challenges and Solutions," 2022, 2–5.

PEMBAHASAN

Reformasi Kelembagaan dan Peningkatan Kapasitas

Salah satu hal yang paling mendesak untuk segera dibenahi adalah kelembagaan BSSN itu sendiri. Jika melihat bagaimana CSA di Singapura atau CISA di Amerika Serikat bekerja, ada pola yang sama, otoritas siber yang efektif butuh mandat hukum yang kuat, anggaran yang cukup, dan kewenangan koordinasi yang tidak tumpang tindih dengan lembaga lain. Model *triple helix* yang melibatkan pemerintah, industri, dan akademisi secara terintegrasi menjadi salah satu pendekatan yang layak dipertimbangkan.

Penguatan Kerangka Hukum dan Standar Teknis

Regulasi yang ada perlu diperkuat dengan aturan turunan yang lebih konkret dan bisa dioperasionalkan. Ini mencakup penetapan standar keamanan minimum yang wajib dipenuhi pengelola infrastruktur kritis, kewajiban melaporkan insiden dalam tenggat waktu tertentu, mekanisme sertifikasi keamanan untuk vendor dan mitra pemerintah, serta insentif bagi organisasi yang serius berinvestasi di bidang keamanan siber.

Kerjasama Publik-Swasta dan Internasional

Proyek-proyek strategis seperti pembangunan Ibu Kota Nusantara tidak bisa dilepaskan dari pertimbangan keamanan siber yang matang meliputi perlindungan data, keamanan informasi strategis, hingga pelibatan publik yang bermakna. Ini menegaskan bahwa ancaman siber bukan urusan teknis semata, melainkan soal tata kelola dan kolaborasi banyak pihak. Dilevel internasional, Indonesia perlu lebih aktif terlibat dalam mekanisme ASEAN-SIRT, mempererat kerjasama bilateral di bidang siber, serta memperkuat partisipasi dalam forum global. Lebih dari itu, Indonesia perlu membangun posisi yang lebih proaktif bukan hanya mengikuti norma yang dibentuk negara lain, tetapi ikut membentuknya.

SIMPULAN

Ancaman siber terhadap infrastruktur kritis Indonesia nyata dan terus berkembang. Masalahnya bukan hanya pada ancaman dari luar, tapi pada kesenjangan yang masih lebar antara regulasi yang ada dengan kemampuan nyata untuk menjalankannya. Insiden PDNS 2024 adalah bukti keras dari kelemahan sistematik yang selama ini mungkin dianggap remeh. Dari sini, ada empat rekomendasi yang perlu ditindaklanjuti secara serius. Pertama, perkuat BSSN dengan mandat hukum yang lebih tegas, anggaran yang sepadan, dan kejelasan kewenangan koordinasi termasuk formalisasi peran TNI *Cyberforce* dalam arsitektur pertahanan siber nasional. Kedua, terbitkan regulasi turunan yang konkret dari UU PDP dan Perpres IIV, lengkap dengan standar teknis, kewajiban pelaporan insiden, dan mekanisme audit berkala. Ketiga, tingkatkan investasi secara signifikan, baik dalam anggaran keamanan siber, pengembangan SDM, maupun pembangunan infrastruktur cadangan data yang benar-benar andal. Keempat, dorong terbentuknya pusat berbagi informasi berbasis sektor (ISAC) dan perkuat keterlibatan Indonesia dalam kerjasama siber regional maupun global. Transformasi digital Indonesia harus terus melaju, tapi di atas fondasi keamanan yang jauh lebih kokoh dari sekarang. Keamanan siber bukan lagi pilihan tapi syarat mutlak bagi kedaulatan digital dan ketahanan nasional Indonesia pada abad ini.

REFERENSI

Bua, I. T., & Idris, N. I. (2025). Analisis kebijakan keamanan siber di Indonesia: Studi kasus kebocoran data nasional pada tahun 2024. *2*, 100–114.

Cloramidine, F., & Badaruddin, M. (2023). Mengukur keamanan siber Indonesia melalui indikator pilar kerjasama dalam *Global Cybersecurity Index* (GCI). *8*, 57–73.

Fifth edition. (n.d.).

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.

Konawe, B., Provins, K., Tenggara, S., Daerah, P., Konawe, K., Nomor, K., Ang, T., Dengan, K., Tuhan, R., Maha, Y., Bupati, E. S. A., Kepulauan, K., Negara, U. D., Indonesia, R., Kepemudaan, U., Daerah, P., & Daerah, P. (2021). *No title*.

Badan Siber dan Sandi Negara. (n.d.). *Laporan kinerja BSSN tahun 2023 (LKJ-BSSN-2023)*.

Maglaras, L., & Janicke, H. (2022). Cybersecurity of critical infrastructures: Challenges and solutions. *2–5*.

Dunn, W. N. (n.d.). *Public policy analysis*.

Sari, M. N. (n.d.). Cybercrime in Association of Southeast Asian Nations: Regional effort and its effectiveness, *14*.

Watney, M. (2021). Cybersecurity threats to and cyberattacks on critical infrastructure: A legal perspective. *319–327*.