Journal of Applied Informatics Science
Open Access: https://doi.org/10.65897/jais.v1.i1.80
Vol. 2, Issue. 1, 2026, pp. 13-18
e-ISSN: 3110-7451

Analysis of National Security Mitigation Strategy Effectiveness Against 2025 Cyber Warfare Escalation

Analisis Efektivitas Strategi Mitigasi Keamanan Nasional terhadap Eskalasi Ancaman Perang Siber Tahun 2025

Rizki Dewantara[1]*, Gina Khayatun Nufus[2] , Eko Jhony Pranata[3], Fariz Noor Djati[4]

[1,2,4] *Informatika, UIN Siber Syekh Nurjati Cirebon, Cirebon, Indonesia,* [3] *Ilmu Komputer, Universitas Wira Buana, Lampung, Indonesia*
[1] dewantararizki@uinssc.ac.id, [2] ginakhn@uinssc.ac.id, [3] masekojhonypranata@gmail.com, [4] farizinformatikaa@gmail.com

ARTICLE INFO

Article history:
Received : 2026-03-13
Revised : 2026-03-30
Accepted : 2026-04-01

Kata Kunci:
Anomali Trafik, Keamanan Nasional, Keamanan Siber, Kedaulatan Digital, Perang Siber

Keywords:
Anomaly Traffic, Cybersecurity, Cyberwarfare, Digital Sovereignty, National Security

This is an open access article under the CC BY-SA license.
Copyright © 2026 by Author. Published by GWS Tech Solution.

ABSTRAK

Kemajuan teknologi internet telah menciptakan interkoneksi global yang memicu ancaman perang siber terhadap keamanan nasional. Masalah utama yang dihadapi Indonesia adalah tingginya kerentanan terhadap serangan digital, dengan catatan 3,64 miliar *anomali* trafik pada awal 2025. Penelitian ini bertujuan untuk menganalisis berbagai jenis, tingkat bahaya, dan dampak serangan siber dalam mengganggu stabilitas kedaulatan negara. Metode penelitian yang digunakan adalah kualitatif *non-interaktif* melalui pengkajian dokumen sekunder dari jurnal ilmiah dan laporan resmi otoritas siber. Hasil penelitian menunjukkan adanya fluktuasi *anomali* trafik yang signifikan dengan puncak tertinggi mencapai 615,4 juta kejadian pada Juni 2025. Tren serangan mulai bergeser dari eksploitasi teknis menuju rekayasa sosial yang menyasar celah psikologis pengguna. Kesimpulannya, Indonesia masih berada dalam kategori negara rentan sehingga diperlukan penguatan regulasi serta peningkatan kapasitas sumber daya manusia untuk menghadapi evolusi ancaman siber.

ABSTRACT

Advances in internet technology have created a global interconnectedness that has sparked the threat of cyberwarfare against national security. The main issue facing Indonesia is its high vulnerability to digital attacks, with 3.64 billion traffic anomalies recorded in early 2025. This study aims to analyze the various types, levels of danger, and impacts of cyberattacks in disrupting the stability of national sovereignty. The research method employed is non-interactive qualitative analysis through a review of secondary documents from scientific journals and official reports from cyber authorities. The results indicate significant fluctuations in traffic anomalies, with the highest peak reaching 615.4 million incidents in June 2025. Attack trends are shifting from technical exploitation toward social engineering that targets users' psychological vulnerabilities. In conclusion, Indonesia remains in the category of vulnerable nations, necessitating strengthened regulations and enhanced human resource capacity to address the evolving cyber threats.

1. PENDAHULUAN

Perkembangan ekonomi digital di Indonesia, termasuk pemanfaatan *big data* dalam sistem *e-commerce*, menuntut kesiapan infrastruktur yang mampu memprediksi tantangan di masa depan [1]. Tantangan ini mencakup perlunya strategi penangkalan (deterrence) yang kuat untuk menghadapi aktor siber yang mengancam kedaulatan negara [2]. Realitas ancaman ini semakin nyata dengan adanya insiden besar seperti serangan *ransomware* "Brain Cipher" yang melumpuhkan sistem vital nasional [3]. Berbagai laporan ancaman digital menunjukkan bahwa skala serangan siber di Indonesia terus meningkat secara signifikan [4]. Bahkan, data terbaru mencatat adanya miliaran serangan siber yang terjadi hanya dalam waktu setengah tahun, menunjukkan intensitas yang sangat tinggi di ruang digital [5].

Kondisi keamanan siber di masa mendatang juga diprediksi akan semakin kompleks dengan munculnya teknologi kecerdasan buatan seperti *AI Agentic* yang dapat digunakan untuk serangan otomatis [6]. Melalui tinjauan lanskap keamanan siber nasional, terlihat bahwa kerentanan sistem masih menjadi isu utama yang harus segera diatasi [7]. Sepanjang tahun 2025, *fluktuasi anomali* trafik siber menunjukkan pola serangan yang dinamis dan berbahaya di setiap bulannya [8]. Oleh karena itu, penetapan rencana strategis yang komprehensif sangat diperlukan sebagai landasan hukum dan panduan teknis pertahanan nasional [9]. Berbagai pemikiran strategis kini diarahkan untuk memetakan potensi perang siber yang dapat mengganggu stabilitas negara [10].

Selain aspek teknis, rendahnya tingkat kesadaran dan perilaku keamanan siber di masyarakat Indonesia masih menjadi celah yang sering dieksploitasi oleh peretas [11].

*Corresponding author.
E-mail addresses: dewantararizki@uinssc.ac.id (First Author)

Hasil evaluasi manajemen keamanan informasi menggunakan *Indeks* KAMI pada berbagai jaringan instansi sering kali menunjukkan bahwa tingkat kematangan sistem masih perlu ditingkatkan [12]. Lemahnya perlindungan ini terbukti pada kasus kebocoran data di Pusat Data Nasional yang memberikan dampak luas pada berbagai layanan publik [13]. Upaya penguatan kedaulatan digital juga harus didukung oleh inovasi berkelanjutan dan riset yang mendalam di bidang teknologi [14]. Pengembangan talenta keamanan siber melalui program pelatihan terstruktur menjadi langkah krusial dalam mencetak tenaga ahli yang siap melindungi data nasional [15].

Potensi ancaman siber yang menyasar bidang ekonomi dapat berdampak buruk pada ketahanan nasional secara keseluruhan jika tidak ditangani dengan serius. Diperlukan analisis mendalam terhadap strategi keamanan nasional untuk memastikan kebijakan yang diambil selaras dengan dinamika ancaman global [17]. Implementasi regulasi seperti UU Pelindungan Data Pribadi (PDP) diharapkan mampu menjadi kerangka hukum yang kuat dalam melindungi hak-hak digital warga negara [18]. Evaluasi risiko secara berkala terhadap infrastruktur digital pemerintah harus terus dilakukan guna memitigasi kemungkinan serangan di masa depan [19]. Pada akhirnya, memahami perang siber sebagai bentuk ancaman keamanan baru yang eksistensial adalah kunci untuk membangun sistem pertahanan nasional yang tangguh di era digital [20]. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis eskalasi ancaman siber internasional terhadap keamanan nasional Indonesia serta mengevaluasi efektivitas strategi mitigasi yang telah diimplementasikan dalam menghadapi tantangan kedaulatan digital di tahun 2025.

2. METODE

Penelitian ini berfokus pada berbagai bentuk ancaman dan serangan siber dari lingkup internasional ke dalam negeri Indonesia, mencakup periode historis hingga kondisi saat ini. Berdasarkan objek penelitian tersebut, dilakukan analisis mendalam mengenai jenis, tingkat bahaya, serta proyeksi dampak serangan siber dalam mengganggu stabilitas keamanan nasional Indonesia. Pemetaan pola serangan ini menjadi krusial mengingat eskalasi ancaman digital yang terus meningkat dan menargetkan infrastruktur kritis serta data nasional.

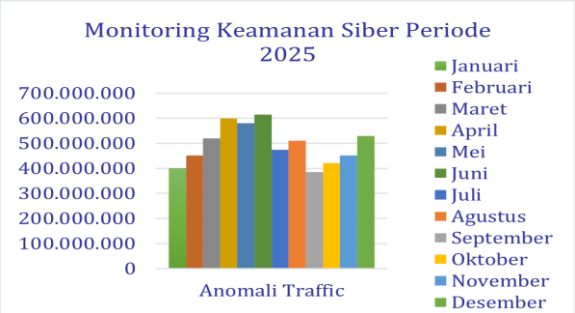
Metode yang digunakan dalam penelitian ini adalah kualitatif non-interaktif. Pendekatan kualitatif sering diklasifikasikan sebagai metode baru, *pospositivistik*, artistik, maupun *interpretive research*, yang diterapkan untuk meneliti pada kondisi objek alamiah di mana peneliti bertindak sebagai instrumen kunci [16]. Secara spesifik, metode kualitatif non-interaktif ini dijalankan melalui penelitian analisis dengan melakukan pengkajian mendalam berdasarkan analisis dokumen. Penelitian ini mengandalkan sumber data sekunder yang dikumpulkan dari berbagai literatur otoritatif, mencakup jurnal ilmiah, laporan resmi otoritas siber, portal berita, situs *web,* serta *e-book* yang membahas dinamika *cyberwar* dan ketahanan keamanan nasional.

3. HASIL DAN PEMBAHASAN

Pada era teknologi yang berkembang pesat saat ini, internet telah bertransformasi menjadi kebutuhan primer yang setara dengan kebutuhan pokok pangan, sandang, dan papan. Ketergantungan masyarakat Indonesia terhadap ruang digital tidak lagi hanya sekadar pilihan, melainkan sebuah keharusan dalam menjalankan roda kehidupan sehari-hari. Transformasi digital yang dipicu oleh pandemi beberapa tahun lalu kini telah mencapai tahap maturitas di berbagai sektor vital, seperti pendidikan yang kini mengadopsi sistem pembelajaran berbasis AI, sektor bisnis yang mengandalkan infrastruktur komputasi awan, hingga sektor perbankan dan perdagangan yang kini menghadapi tantangan keamanan siber yang jauh lebih kompleks dibandingkan tahun-tahun sebelumnya.

Namun, integrasi digital yang semakin dalam ini berbanding lurus dengan peningkatan risiko keamanan nasional yang signifikan. Sepanjang tahun 2025, intensitas serangan siber mencapai level yang sangat mengkhawatirkan. Berdasarkan data dari Bloomberg Technoz, Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 3,64 miliar serangan siber terjadi hanya dalam kurun waktu Januari hingga Juli 2025. Data monitoring bulanan BSSN tahun 2025 menunjukkan bahwa trafik *anomali* terus ber*fluktuasi* dengan rata-rata di atas 400 juta per bulan, di mana puncak *anomali* tertinggi terjadi pada bulan Juni 2025 yang mencapai angka 615.430.700 kejadian.

Pola ancaman siber pada tahun 2025 juga menunjukkan pergeseran ke arah serangan yang lebih terstruktur dan destruktif. Jika sebelumnya gangguan didominasi oleh hoaks dan pencurian data sederhana, kini Indonesia menghadapi ancaman yang menargetkan kedaulatan infrastruktur kritis nasional. Insiden besar seperti serangan *ransomware* "Brain Cipher" yang melumpuhkan Pusat Data Nasional (PDN) pada tahun 2025 menjadi bukti nyata kerentanan manajemen risiko keamanan siber pada instansi pemerintah. Selain itu, munculnya ancaman berbasis kecerdasan buatan seperti AI *Agentic* yang mampu melakukan serangan otomatis secara mandiri menambah daftar tantangan baru bagi ketahanan nasional. Realitas ini menunjukkan bahwa masyarakat tidak hanya menciptakan dunia baru yang berdampingan dengan dunia nyata, tetapi juga medan pertempuran baru yang memerlukan sistem pertahanan siber yang lebih proaktif dan responsif di masa depan [5].



Gambar 1. Diagram Monitoring Keamanan Siber 2025

Sepanjang tahun 2025 yang ditunjukkan pada Gambar 1,

trafik *anomali* siber menunjukkan dinamika yang sangat intens dengan total mencapai 3,64 miliar serangan selama periode Januari hingga Juli. Puncak *anomali* tahunan terjadi pada bulan Juni sebanyak 615.430.700 kejadian yang didominasi oleh upaya serangan *Ransomware* dan *Brute Force*. Perjalanan ancaman ini dimulai dengan eksploitasi infrastruktur melalui *Mirai Botnet* pada bulan Januari (400,1 juta *anomali*) dan serangan DDoS di bulan Februari (450,7 juta), lalu bertransformasi menjadi risiko pencurian data melalui SQL *Injection* pada bulan April (600,2 juta) serta pencurian kredensial di bulan Mei (580,9 juta). Meskipun sempat mengalami penurunan *volume* terendah pada bulan September yang mencapai 386,1 juta *anomali*, munculnya lonjakan *Trojan* yang sangat tajam pada tanggal 28 September serta penggunaan *Zero-Day Exploit* pada bulan Oktober (420,5 juta) membuktikan bahwa peretas tetap aktif meluncurkan serangan terukur. Menjelang akhir tahun, strategi peretasan beralih ke aspek manusia melalui kampanye *Phishing* pada bulan November (450,8 juta) dan *Social Engineering* yang ditutup dengan upaya eksfiltrasi data pada bulan Desember (530,1 juta), memberikan gambaran bahwa ancaman siber tahun 2025 kini tidak hanya menyerang sistem secara teknis tetapi juga memanfaatkan celah psikologis pengguna secara konsisten yang dapat dilihat pada Tabel 1.

Tabel 1. Tabel Monitoring Keamanan Siber 2025

	Anomali Traffic	Serangan Tertinggi	*Anomali* Tertinggi
Januari	400.125.600	Malware Activity	Mirai Botnet
Februari	450.780.200	DDoS Attack	DNS Amplification
Maret	520.440.900	Web Defacement	Malicious URL
April	600.210.330	Data Breach	SQL *Injection*
Mei	580.990.110	Credential Theft	Unauthorized Access
Juni	615.430.700	*Ransomware* Attempt	*Brute Force*
Juli	475.220.550	Botnet Traffic	Exploit Kit
Agustus	510.660.880	Malware *Injection*	IoT Vulnerability
September	386.110.220	*Trojan* Activity	20.6M Spike
Oktober	420.550.990	Zero-Day Exploit	Backdoor Access
November	450.880.330	*Phishing* Campaign	C2 Communication
Desember	530.120.440	*Social Engineering*	Data Exfiltration

Berdasarkan Tabel 1, peningkatan penggunaan internet di Indonesia tidak hanya mendorong kemajuan ekonomi, tetapi juga berdampak signifikan pada peningkatan intensitas serangan siber. Hal ini memperbesar potensi terjadinya perang siber antarnegara maupun serangan oleh aktor non-negara yang dapat mengganggu kedaulatan nasional. Berdasarkan perkembangan terbaru hingga tahun 2025, terdapat beberapa insiden siber krusial yang memengaruhi stabilitas nasional:

- Kasus Pusat Data Nasional (PDN): Serangan *ransomware* "Brain Cipher" pada tahun 2025 melumpuhkan infrastruktur digital pemerintah dan mengakibatkan gangguan layanan publik yang masif.
- Kebocoran Data Nasional: Analisis terhadap kebocoran data pada Pusat Data Nasional Sementara (PDNS) 2 Surabaya menunjukkan kerentanan sistem penyimpanan data nasional yang berdampak luas pada keamanan informasi warga negara.
- Keamanan Perbankan Digital: Sektor ekonomi dan perbankan, seperti kasus perlindungan nasabah Bank Syariah Indonesia (BSI), menjadi sorotan utama terkait risiko kebocoran data yang dapat menurunkan tingkat kepercayaan masyarakat terhadap ekosistem digital.

Rentetan insiden ini membuktikan bahwa potensi *cyberwar* di era transformasi digital semakin besar, terutama dengan munculnya ancaman baru seperti AI Agentik yang mampu melakukan serangan otomatis secara mandiri. Oleh karena itu, pemerintah memerlukan *elemen* perlindungan siber yang komprehensif untuk menjamin rasa aman bagi seluruh warga negara.

3.1 Strategi Keamanan Siber Indonesia

Keamanan siber didefinisikan sebagai upaya menjaga kerahasiaan, integritas, dan ketersediaan informasi di ruang siber melalui praktik perlindungan sistem dan jaringan. Indonesia mengadopsi lima bidang kerja *Global Cyber-Security* dalam strategi pertahanannya :

- Kepastian Hukum: Indonesia telah memperkuat landasan hukum melalui implementasi UU Pelindungan Data Pribadi (PDP) serta Peraturan BSSN Nomor 8 Tahun 2025 tentang Rencana Strategis BSSN untuk memastikan kesiapan menghadapi ancaman masa depan.
- Teknis dan Tindakan Prosedural: Pemanfaatan kecerdasan buatan (AI) kini menjadi solusi utama dalam meningkatkan kemampuan deteksi dan respons terhadap serangan siber secara *real-time*.
- Struktur Organisasi: Pembentukan dan penguatan struktur Badan Siber dan Sandi Negara (BSSN) bertujuan untuk membangun sistem pertahanan siber yang universal dan terintegrasi di seluruh instansi pemerintah.
- Capacity Building: Peningkatan kualitas SDM dilakukan melalui program pelatihan seperti *Ready4Security* bagi talenta digital serta pelatihan keamanan jaringan pada tingkat pendidikan menengah kejuruan untuk membangun resiliensi siber sejak dini.
- Kerjasama Internasional: Indonesia aktif menjalin kolaborasi bilateral dan multilateral, termasuk melalui forum ASEAN *Defence Ministers' Meeting* (ADMM-Plus), untuk memperkuat pertahanan siber di kawasan regional.

Meskipun strategi telah dijalankan, tantangan tetap besar mengingat BSSN mencatat adanya 3,64 miliar serangan siber sepanjang periode Januari hingga Juli 2025 [5]. Hal ini menunjukkan bahwa Indonesia masih berada dalam posisi yang rentan, sehingga penguatan koordinasi

dan edukasi pengguna internet secara konsisten menjadi syarat mutlak dalam menjaga kedaulatan ruang siber nasional.

3.2 Analisis dan Mitigasi Keamanan Siber di Indonesia

Peningkatan penggunaan internet di Indonesia tidak hanya mendorong kemajuan ekonomi, tetapi juga berdampak signifikan pada peningkatan intensitas serangan siber.

Tabel 2. Tabel Analisis dan Mitigasi Keamanan Siber di Indonesia

Entitas	Tahun/ Periode	Jenis Insiden atau Tantangan	Dampak Insiden	Langkah Strategis atau Mitigasi	Status atau Hasil Implementasi
Perusahaan Listrik Negara (PLN)	2019	Pemadaman listrik (akibat ketergantungan teknologi digital)	Kerugian finansial sebesar Rp 90 Miliar ditambah pembayaran kompensasi pelanggan.	Pemerintah menyiapkan infrastruktur (listrik dan internet) serta pengembangan SDM.	Data kerugian dilaporkan secara resmi.
Pemerintah Indonesia (Sektor Administrasi)	2024	*Anomali* dan serangan siber (dominan Data Breach)	Sektor Administrasi Pemerintah menjadi yang paling banyak terdampak masalah keamanan siber sepanjang 2024.	Pengiriman 1.367 notifikasi indikasi insiden oleh BSSN kepada pemangku kepentingan.	58% notifikasi direspon oleh stakeholder; 42% tidak direspon.
Pusat Data Nasional Sementara (PDNS) 2 Surabaya	Juni 2024	Serangan *Ransomware* (Varian Brain Cipher/LockBit 3.0)	Melumpuhkan lebih dari 210 lembaga pemerintah; layanan publik kritis (imigrasi, pendaftaran siswa) terhenti; pemerasan US$ 8 juta.	Evaluasi manajemen risiko, penerapan strategi cadangan data 3-2-1, dan audit keamanan ketat.	Pemerintah secara tegas menolak membayar tebusan; pemulihan data sempat mustahil karena ketiadaan cadangan yang terisolasi.
Bank Syariah Indonesia (BSI)	Mei 2023	Serangan Ransomware	Gangguan operasional harian jutaan nasabah; penurunan kepercayaan publik; *fluktuasi* negatif harga saham; kerugian moneter mencapai Rp 10 triliun.	Alokasi belanja modal (Capex) keamanan sebesar Rp 580 miliar untuk penguatan sistem.	Penguatan ketahanan sistem dan perlindungan data nasabah dilakukan pasca-serangan.
Dukcapil	2023-2024	Kebocoran Data Massal	337 juta rekaman data pribadi (NIK, informasi keluarga) bocor melalui BreachForums; peningkatan kasus penipuan identitas.	Pengesahan dan pemberlakuan penuh UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).	UU PDP mulai berlaku sepenuhnya pada Oktober 2024.
Pemerintah Indonesia (Nasional)	2024-2025	Kesenjangan Talenta Keamanan Siber	Kekurangan signifikan tenaga ahli; kesenjangan kurikulum akademis dengan kebutuhan industri.	Program Ready4Security, penyediaan Cyber Range untuk simulasi, dan kolaborasi universitas-industri.	BSSN bekerja sama dengan Google Cloud memberikan 1.000 beasiswa sertifikat keamanan siber.
Sektor Perbankan dan Fintech	2025 (Prediksi)	Teknologi Deepfake	Pemalsuan identitas wajah dalam proses onboarding digital; kerugian rata-rata US$ 250.000 per insiden.	Implementasi sistem deteksi 'liveness' yang tangguh dan AI sebagai solusi deteksi ancaman.	Masih dalam tahap pengembangan dan promosi oleh pemerintah.
Instansi Pemerintah Daerah (Bali, Jatim, Jateng, dll)	2024	Celah Keamanan Sistem Elektronik (Vulnerability)	Ditemukan 1.931 kerentanan (256 kritikal) pada 462 aplikasi yang diuji.	Layanan IT Security Assessment (ITSA) dan Voluntary Vulnerability Identification and Protection (VVIP) Program (Bug Hunter).	Stakeholder dapat segera memperbaiki celah kerentanan yang ditemukan oleh para bug hunter.
Pusat Data Nasional Sementara (PDNS) 2 Surabaya	Juni 2024	*Ransomware* Braincipher (varian Lockbit 3.0)	Gangguan pada 282 instansi layanan publik termasuk layanan keimigrasian, kerugian finansial yang signifikan, dan tuntutan tebusan USD 8 juta.	Implementasi strategi backup 3-2-1, audit keamanan siber, aktivasi CSIRT, serta pemulihan melalui tiga zona (merah, biru, hijau).	Pemulihan layanan dilakukan melalui backup server cold site BTAM; reaktivasi layanan di fasilitas PDNS 1.
Bank Syariah Indonesia (BSI)	Mei 2023	Serangan *Ransomware* (LockBit 3.0) dan gangguan sistem.	Layanan ATM, mobile banking, dan teller lumpuh selama beberapa hari; penurunan harga saham BRIS; pencurian 1,5 terabyte data nasabah.	Alokasi belanja modal Rp 580 miliar untuk keamanan data, penggunaan otentikasi dua faktor, enkripsi data, dan koordinasi dengan BSSN, OJK, serta BI.	Normalisasi layanan dilakukan bertahap; rasio keuangan (KPMM, ROA, ROE) tetap sehat meskipun rasio FDR menurun.
Sektor Pendidikan	2024	Kesenjangan talenta keamanan siber dan ketidaksesuaian kurikulum	Kekurangan tenaga ahli (kebutuhan 50.000, tersedia 8.000); lulusan kesulitan	Memasukkan mata kuliah keamanan siber ke prodi umum, merancang program	Program Ready4Security telah melatih lebih dari 1.750

(Universitas)		dengan kebutuhan industri.	beradaptasi dengan dunia kerja.	pelatihan praktis, program magang, dan inisiatif seperti Ready4Security.	peserta dari SMK dan Perguruan Tinggi.
Pemerintah Indonesia (Kemenkominfo/BSSN)	2023-2025	*Anomali* trafik siber (3,64 miliar serangan) dan ancaman AI Agentik.	Kerugian ekonomi siber mencapai Rp18 triliun pada 2024; risiko penipuan deepfake dan *Phishing* berbasis AI.	Penggunaan AI untuk deteksi ancaman, pembentukan Lembaga Perlindungan Data Pribadi (PDP), dan percepatan RUU Keamanan dan Ketahanan Siber.	Kerja sama strategis BSSN dengan Google untuk pelatihan 1.000 beasiswa Google Cybersecurity Certificate.
BPJS Kesehatan	April 2025	Kebocoran data massal.	Kebocoran 40 juta data peserta.	Langkah mitigasi siber oleh otoritas terkait.	Berhasil diatasi.
Bank Sentral Indonesia	Mei 2025	Serangan *Phishing* massal.	Sistem digital bank lumpuh selama 12 jam.	Penguatan prosedur keamanan internal.	Sistem berhasil dipulihkan.

Berdasarkan data dari Tabel 2, dapat dipetakan bahwa kedaulatan digital nasional sangat bergantung pada sinkronisasi antara aspek hukum, teknologi, dan sumber daya manusia. Indonesia telah memperkuat landasan hukum melalui implementasi UU Pelindungan Data Pribadi (PDP) serta Peraturan BSSN Nomor 8 Tahun 2025. Lanskap keamanan siber nasional sepanjang tahun 2025 menunjukkan eskalasi yang sangat masif dan mengkhawatirkan. Tercatat total *anomali* trafik mencapai angka 3,64 miliar serangan selama periode Januari hingga Juli 2025, yang mencerminkan tingginya intensitas aktivitas peretasan terhadap ruang siber Indonesia. Puncak *fluktuasi* serangan terjadi pada bulan Juni dengan *volume* mencapai 615,4 juta kejadian, di mana jenis serangan didominasi oleh aktivitas *Ransomware* dan *Brute Force*.

Fenomena ini mengonfirmasi teori *interdependensi* digital, di mana keterhubungan infrastruktur yang semakin dalam justru memperluas permukaan serangan (attack surface) bagi aktor siber. Penurunan *volume anomali* sempat terpantau pada bulan September menjadi 386,1 juta, namun kemunculan lonjakan tajam aktivitas *Trojan* pada akhir bulan tersebut serta penggunaan *Zero-Day Exploit* pada bulan Oktober membuktikan bahwa ancaman tetap bersifat persisten dan terukur.

3.3. Transformasi Metodologi dan Pola Serangan

Analisis terhadap pola serangan mengungkap adanya pergeseran strategi dari eksploitasi infrastruktur teknis menuju eksploitasi celah psikologis pengguna. Pada kuartal pertama 2025, ancaman difokuskan pada gangguan ketersediaan layanan melalui *Mirai Botnet* dan serangan DDoS. Memasuki pertengahan tahun, peretas mulai menargetkan kerahasiaan data melalui teknik SQL *Injection* dan pencurian kredensial.

Transformasi paling signifikan terlihat pada akhir tahun 2025, di mana strategi penyerangan beralih ke kampanye *Phishing* dan *Social Engineering*. Hal ini menunjukkan bahwa aktor siber semakin menyadari bahwa faktor manusia sering kali menjadi rantai terlemah dalam sistem keamanan digital nasional. Selain itu, integrasi kecerdasan buatan dalam bentuk AI *Agentic* telah mempercepat kemampuan peretas dalam meluncurkan serangan otomatis yang sulit dideteksi oleh sistem pertahanan konvensional meskipun instrumen hukum seperti UU PDP telah diimplementasikan, besarnya angka serangan sebesar 3,64 miliar pada semester pertama 2025 menunjukkan bahwa efektivitas regulasi tersebut masih memerlukan dukungan infrastruktur teknis yang lebih *responsif*. Hal ini mengindikasikan adanya celah antara kebijakan *administratif* dengan kesiapan operasional di lapangan.

4. SIMPULAN

Berdasarkan analisis yang telah dilakukan, dapat disimpulkan bahwa *efektivitas* strategi *mitigasi* keamanan nasional Indonesia pada tahun 2025 masih berada pada *level* yang perlu diakselerasi secara *signifikan*. Meskipun pemerintah telah menetapkan landasan *regulatif* yang kuat melalui UU Pelindungan Data Pribadi dan Rencana Strategis BSSN 2025, data menunjukkan adanya disparitas antara kebijakan administratif dengan ketahanan teknis di lapangan. Rekor 3,64 miliar serangan siber selama periode Januari hingga Juli 2025, dengan puncak anomali mencapai 615,4 juta kejadian, menjadi bukti empiris bahwa strategi mitigasi yang ada belum mampu meredam laju eskalasi ancaman perang siber yang bersifat asimetris dan masif.

Penelitian ini menemukan bahwa titik lemah efektivitas mitigasi terletak pada belum optimalnya resiliensi infrastruktur kritis, sebagaimana terkonfirmasi pada insiden ransomware "Brain Cipcher" di Pusat Data Nasional. Serangan tersebut menegaskan bahwa perlindungan hukum dan kerja sama internasional seperti forum ADMM-Plus tidak akan mencapai efektivitas maksimal tanpa didukung oleh sistem pertahanan proaktif dan audit keamanan teknis yang berkelanjutan. Efektivitas pertahanan masa depan sangat bergantung pada kemampuan Indonesia dalam mengintegrasikan teknologi kecerdasan buatan, seperti sistem deteksi dini untuk menangkal AI *Agentic*, serta penguatan kapasitas talenta digital dalam memitigasi serangan berbasis rekayasa sosial.

Sebagai rekomendasi strategis, pengembangan penelitian selanjutnya perlu diarahkan pada penguatan kedaulatan digital melalui penerapan *kriptografi* pasca-kuantum dan optimalisasi *resiliensi* siber berbasis kemandirian teknologi. Hal ini krusial untuk memastikan bahwa strategi mitigasi tidak hanya bersifat reaktif, namun mampu memberikan jaminan keamanan nasional yang tangguh di tengah korelasi interdependensi ruang digital global yang terus berevolusi.

DAFTAR PUSTAKA

[1] A. P. Yanuar, "Cyber War: Ancaman Baru Keamanan Nasional dan Internasional," Jurnal Keamanan Nasional, vol. VII, no. 1, pp. 23-35, 2021.

[2] I. K. Rahakbauw dan I. A. Batubara, "Analisis Potensi Ancaman Siber pada Bidang Ekonomi di Indonesia," Jurnal Kajian Stratejik Ketahanan Nasional, vol. 7, no. 1, 2024.

[3] B. A. Darumaya, S. Maarif, T. S. L. Toruan, dan Y. Swastanto, "Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan," Jurnal Keamanan Nasional, vol. 9, no. 2, pp. 299-324, 2023.

[4] Bloomberg Technoz, "BSSN Catat 3,64 Miliar Serangan Siber Selama Januari-Juli 2025," 2025.

[5] BSSN, Badan Siber dan Sandi Negara, Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Bulan Januari - Desember 2025, Jakarta, 2025.

[6] BPIP-CSIRT, "Ancaman Siber 2025: Indonesia Harus Waspada AI Agentik," 2025.

[7] I. Armansyah, Y. Tabrani, M. S. Khoir, D. W. Putra, dan A. E. Augustia, "Studi Kasus Serangan *Ransomware* Brain Cipher pada Pusat Data Nasional Indonesia," BIN: Bulletin Of Informatics, vol. 3, no. 1, pp. 85-89, 2025.

[8] S. Tommy dan M. I. P. Nasution, "Evaluasi Manajemen Risiko Keamanan Siber Pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN)," Jurnal Manajemen Ekonomi dan Bisnis, vol. 4, no. 1, 2025.

[9] E. R. M. Sembiring, N. Nurbaiti, dan A. N. Daulay, "Pengaruh Ancaman Siber *Ransomware* dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran," Jurnal Manajemen Pendidikan dan Ilmu Sosial, vol. 5, no. 4, pp. 880-887, 2024.

[10] R. Dewantara dan B. Sugiantoro, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 8, no. 6, pp. 1137-1148, 2021.

[11] SGU, "From Policy to Practice: How Indonesia's UU PDP 2022 Shapes Cybersecurity Readiness 2025," Swiss German University.

[12] BSSN, "Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 8 Tahun 2025 Tentang Rencana Strategis Badan Siber dan Sandi Negara," 2025.

[13] L. Judijanto dan R. Dewantara, "Visualisasi Domain Pengetahuan dan Analisis Tren Riset dalam Bidang Inovasi Berkelanjutan," Sanskara Ekonomi dan Kewirausahaan, vol. 4, no. 1, pp. 51–63, 2025.

[14] InfoKomputer, "Keamanan Siber APAC 2026: Tantangan Kuantum, AI, dan Ketahanan Digital," 2026.

[15] Microsoft Source, "Jawab Kebutuhan Talenta Keamanan Siber, Peserta Program Ready4Security Berhasil Rancang Solusi Keamanan Siber di Kompetisi U-Connect," 2024.

[16] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif dan R&D, Bandung: Alfabeta, 2019.

[17] K. E. A. Tampubolon, "Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare," Jurist-Diction, vol. 2, no. 2, p. 539, 2019.

[18] R. Dewantara dan D. Rizky April Yadi, "Studi Perbandingan Kesadaran, Pengetahuan, Dan Perilaku Cyber Security Di Indonesia," The Journal Implementation of Data Science, vol. 1, no. 1, 2023.

[19] R. Dewantara, E. J. Pranata, dan U. Latifah, "Peningkatan Keamanan Jaringan Sekolah Melalui Pelatihan Cyber Security di SMK 7 PURWOREJO," Jurnal Pengabdian Kepada Masyarakat IBISA, vol. 2, no. 2, pp. 7–12, 2024.

[20] D. F. Putri, Andriani, W. R. Sari, dan F. L. Nabbila, "Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking," Jurnal Ilmiah Ekonomi dan Manajemen, vol. 1, no. 4, pp. 173-181, 2023.