GOVERNANCE: Jurnal Ilmiah Kajian Politik Lokal dan Pembangunan
ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 13 Nomor 2 Februari 2026

TANTANGAN CYBER DEFENSE DALAM MENGHADAPI SERANGAN SIBER TERHADAP INFRASTRUKTUR PEMERINTAH DI INDONESIA

Callista Diandra Athaillah[1], Devita Larasati Tupen[2], Alya Julianti Sari[3], Fadhia Chalisha Adzzahra[4], Jerry Indrawan[5]
[1,2,3,4,5]Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Pembanngunan Nasional "Veteran" Jakarta
Email Korespondensi: 2310413150@mahasiswa.upnvj.ac.id
Email: 2310412082@mahasiswa.upnvj.ac.id; 2310413150@mahasiswa.upnvj.ac.id; 2310412236@mahasiswa.upnvj.ac.id; 2310413158@mahasiswa.upnvj.ac.id; jerry.indrawan@upnvj.ac.id

ABSTRACT
The massive digital transformation in Indonesia's government sector has presented new challenges in maintaining the security of national cyber infrastructure. Although digitization brings efficiency and transparency in the delivery of public services, it also expands the potential for cyber attacks that could threaten the stability and vital functions of the state. The research method used was a qualitative approach with a literature study oriented towards in-depth analysis of various scientific sources, government regulations, and official reports from institutions such as the National Cyber and Crypto Agency (BSSN). The data was analyzed using content analysis techniques to interpret patterns, trends, and challenges in the national cyber defense system. The results of the study show that Indonesia experienced a significant surge in cyber attacks with 3.64 billion traffic anomalies recorded from January to July 2025.
Keywords: cyber security, e-government, digital infrastructure, BSSN.

ABSTRAK
Transformasi digital yang masif di sektor pemerintahan Indonesia telah menghadirkan tantangan baru dalam menjaga keamanan infrastruktur siber nasional. Meskipun digitalisasi membawa efisiensi dan transparansi dalam penyelenggaraan layanan publik, hal ini juga memperluas potensi serangan siber yang dapat mengancam stabilitas dan fungsi vital negara. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan jenis studi literatur yang berorientasi pada analisis mendalam terhadap berbagai sumber ilmiah, regulasi pemerintah, serta laporan resmi lembaga seperti Badan Siber dan Sandi Negara (BSSN). Data dianalisis menggunakan teknik *content analysis* untuk menafsirkan pola, kecenderungan, dan tantangan dalam sistem pertahanan siber nasional. Hasil penelitian menunjukkan bahwa Indonesia mengalami lonjakan signifikan serangan siber dengan 3,64 miliar anomali trafik tercatat pada Januari–Juli 2025.
Kata kunci: keamanan siber, e-government, infrastruktur digital, BSSN.

PENDAHULUAN
Digitalisasi layanan publik dan transformasi sistem pemerintahan di Indonesia telah mengubah cara penyelenggaraan administrasi, data, dan layanan publik dari manual menjadi berbasis *online.* Ketergantungan pada sistem digital ini membuat keseluruhan arsitektur pemerintahan menjadi rentan terhadap ancaman siber: ketika mekanisme pertahanan tidak memadai, gangguan dapat mempengaruhi integritas data, ketersediaan layanan publik, serta kepercayaan masyarakat terhadap pemerintah. Ancaman tersebut tidak lagi bersifat hipotesis; penelitian terbaru menunjukkan bahwa volume serangan siber terhadap institusi pemerintahan dan infrastruktur kritis di Indonesia meningkat secara signifikan dalam beberapa tahun terakhir, menandakan bahwa kerentanan sistem informasi publik terus menjadi persoalan

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 13 Nomor 2 Februari 2026

serius (Syawaluddin, 2025). Situasi ini diperparah oleh kondisi kerangka regulasi dan implementasi kebijakan keamanan siber nasional yang masih menghadapi tantangan struktural mulai dari fragmentasi lembaga, alokasi anggaran yang minim, hingga lemahnya koordinasi antar instansi dan rendahnya kapasitas sumber daya manusia dalam mengelola *cyber defense* (Alfath & Cahya, 2024; Rusydi, 2025). Efeknya, meskipun regulasi sudah dibentuk, efektivitas pertahanan siber pemerintah cenderung belum optimal, terutama dalam menghadapi ancaman modern seperti *ransomware, malware,* dan serangan terhadap infrastruktur digital kritis (Alfath & Cahya, 2024; Maharani, 2025).

Lebih jauh, transformasi digital yang berlangsung cepat termasuk integrasi layanan publik, penyimpanan data berskala besar, dan konektivitas lintas instansi meningkatkan kompleksitas ancaman dan memperluas permukaan serangan. Kerentanan ini menunjukkan bahwa membangun cyber defense bukan hanya soal teknis proteksi jaringan atau firewall, tetapi memerlukan pendekatan multidimensi: regulasi yang adaptif, koordinasi kelembagaan, pengembangan kapasitas SDM, dan strategi mitigasi serta respons yang siap pakai. Namun, literatur yang mengkaji secara komprehensif tantangan-tantangan ini dalam konteks pemerintahan Indonesia khususnya dari perspektif kesiapan kelembagaan dan tata kelola masih relatif terbatas.

Dengan latar tersebut, penelitian ini bermaksud mengeksplorasi tantangan utama dalam membangun pertahanan siber pada infrastruktur pemerintahan di Indonesia. Fokus analisis diarahkan pada tiga aspek: (1) kerentanan struktural dan kelemahan regulasi, (2) kapasitas kelembagaan dan teknis keamanan siber, serta (3) dinamika implementasi kebijakan dan respons terhadap insiden siber. Dengan demikian, penelitian ini diharapkan memberikan gambaran empiris tentang kondisi aktual cyber defense pemerintahan, sekaligus menawarkan rekomendasi kebijakan untuk memperkuat ketahanan digital nasional.

METODE

Metode penelitian ini menggunakan pendekatan kualitatif dengan jenis studi literatur yang berorientasi pada analisis mendalam terhadap berbagai sumber ilmiah terkait tantangan *cyber defense* dalam menghadapi serangan siber terhadap infrastruktur pemerintah di Indonesia. Studi literatur ini berorientasi pada pencarian, penelaahan, dan analisis mendalam terhadap hasil penelitian terpublikasi, regulasi pemerintah dan kebijakan public. Pemilihan pendekatan ini dilakukan untuk memperoleh pemahaman interpretatif terhadap pola ancaman, kelemahan sistem, serta strategi pertahanan digital nasional (Widiyasono, 2024). Bersifat empiris dan sistematis, dengan tujuan untuk mengidentifikasi pola, kecenderungan, dan tantangan utama dalam sistem pertahanan siber pemerintah Indonesia berdasarkan literatur yang valid dan terkini. Data yang diperoleh dari berbagai sumber kemudian dianalisis menggunakan teknik analisis isi (content analysis) yang memungkinkan peneliti menafsirkan makna dari data tekstual secara sistematis melalui proses kategorisasi dan interpretasi tematik (Bowen, 2009). Proses pengolahan dan analisis data dilakukan secara bertahap, dimulai dari tahap reduksi data, penyajian data, hingga penarikan kesimpulan secara deskriptif (Miles, Huberman, & Saldaña, 2014). Setiap temuan dari literatur diverifikasi untuk memastikan keabsahan dan relevansi terhadap fokus penelitian.

PEMBAHASAN

Bagian ini menyajikan hasil analisis dari studi literatur yang berfokus pada tantangan utama dalam memperkuat *cyber defense* terhadap infrastruktur digital pemerintah indonesia. Analisis ini dilakukan berdasarkan data dan temuan dari berbagai sumber ilmiah serta laporan resmi seperti Badan Siber dan Sandi Negara (BSSN), dengan tujuan memberikan gambaran yang jelas mengenai tingkat kerentanan dan kesiapan nasional dalam menghadapi ancaman siber (Bhakti et al., 2024; Ginting et al., 2023). Berdasarkan data BSSN tahun 2025, tercatat sebanyak 3,64 miliar serangan siber atau anomali trafik terjadi sepanjang Januari hingga Juli 2025, dengan jenis serangan yang paling dominan adalah *Generic Protocol Command Decode* sebesar 68,37 persen. Angka ini menunjukkan peningkatan signifikan dibandingkan dengan tahun

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 13 Nomor 2 Februari 2026

2024 yang mencatat 330,5 juta insiden (BSSN, 2024). Salah satu serangan paling menonjol adalah *Ransomware LockBit 3.0* dan *Brain Cipher* yang melumpuhkan Pusat Data Nasional Sementara (PDNS) dan mengganggu lebih dari 200 layanan publik, termasuk sistem imigrasi dan e-visa (Badan Siber dan Sandi Negara (BSSN). (2025).

Fenomena tersebut menggambarkan bahwa meskipun transformasi digital telah meningkatkan efisiensi dan transparansi layanan publik, di sisi lain juga memperluas *attack surface* yang dapat dieksploitasi oleh aktor jahat baik dari dalam maupun luar negeri. Hal ini menegaskan adanya paradoks digitalisasi, dimana kemajuan teknologi justru menciptakan bentuk kerentanan baru terhadap fungsi vital negara. Selain itu, hasil analisis literatur menunjukkan beberapa faktor penyebab utama masih lemahnya ketahanan siber indonesia, antara lain:

1. Keterbatasan sumber daya manusia dan infrastruktur keamanan siber, khususnya di instansi pemerintah daerah.
2. Kurangnya koordinasi antar lembaga dalam sistem deteksi dini dan penanganan insiden siber.
3. Belum optimalnya implementasi kebijakan nasional keamanan siber yang terintegrasi dengan sistem pemerintah digital *(e-government)*
4. Rendahnya kesadaran keamanan digital *(cyber hygiene)* di kalangan aparatur negara dan pengguna sistem pemerintahan.

Namun demikian, pemerintah Indonesia telah menunjukkan upaya adaptif melalui pembentukan *Computer Security Incident Response Team (CSIRT)* di berbagai instansi, serta peningkatan kerja sama internasional dalam bidang keamanan siber. Strategi penguatan *cyber defense* juga mulai diarahkan pada pendekatan *multi-layered defense* yang menekankan pada kombinasi aspek teknologi, regulasi, dan edukasi publik. Secara keseluruhan, hasil studi ini memperlihatkan bahwa penguatan keamanan siber indonesia tidak hanya bergantung pada teknologi, tetapi juga pada sinergi kelembagaan, tata kelola digital yang kuat, serta peningkatan kapasitas sumber daya manusia yang memahami dinamika ancaman di ruang siber global.

Faktor penyebab lemahnya ketahanan siber Indonesia

Hasil analisis literatur mengidentifikasi beberapa peyebab utama mengapa pertahanan siber Indonesia masih menghadapi tantangan besar:

1. Keterbatasan Sumber Daya Manusia dan Infrastruktur

Banyak instani pemerintahan, terutama di tingkat daerah, belum memiliki tenaga ahli khusus keamanan siber (*cyber security specialist*). Infrstruktur pendukug seperti sistem *intrusion detection*, enkripsi, segmentasi jaringan, dan fasilitas pemantauan real-time masih minim dan tidak merata.

2. Kurangnya Koordinasi Antar Lembaga

Respons terhadap insiden siber sering terlambat karena koordinasi lintas lembaga belum optimal. Perbedaan standar keamanan, alur pelaporan, serta belum adanya pusat koordinasi nasional yang bekerja 24/7 menghambat tindakan cepat saat terjadi serangan besar.

3. Implementasi Kebijakan Keamanan Siber yang Belum Menyeluruh

Kebijakan nasional sebenarnya sudah dirumuskan, namun implementasinya belum merata di seluruh instansi. Banyak lembaga yang belum menerapkan arsitektur *zero trust*, audit keamanan berkala, ataupun manajemen risiko digital yang sistematis.

4. Rendahnya Kesadaran Keamanan Digital (Cyber Hygiene)

Human error masih menjadi penyebab dominan banyak insiden, terasuk phishing, kebocoran kata sandi, dan kesalahan konfigrasi sistem. Literasi keamanan digital aparatur negara masih rendah sehingga celah-celah administratif mudah dieksploitasi.

Upaya Pemerintah dan Perkembangan Strategi Cyber Defense

Meskipun menghadapi tantangan besar, pemerintah Indonesia telah menunjukkan langkah progresif

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 13 Nomor 2 Februari 2026

dalam memperkuat pertahanan siber, antara lain:

- Pembentukan CSIRT di berbagai instansi pemerintah pusat maupun daerah sebagai garda depa penanganan insiden.
- Peningkatan kerja sama internasional dengan BIG, negara sahabat, dan organisasi keamanan global untuk pertukaran informas ancaman (*threat intelligence sharing*).
- Pengembangan strategi multi-layered defense yang menekankan kombinasi teknologi, perlindungan data, regulasi, dan edukasi publik.
- Peningkatan standar tata kelola data, termasuk kewajiban backup, manajemen risiko, dan penggunaan layanan cloud nasional yang lebih aman.
- Simulasi serangan siber (cyber drill) secara berkala untuk melatih kesiapsiagaan instansi dalam merespons insiden.

Upaya ini menunjukkan adanya komitmen negara dalam memperkuat sistem keamanan nasional seiring meningkatnya ketergantungan pada teknologi digital. (Sulubara et al., 2025).

Analisis Kesiapan Nasional dalam Menghadapi Ancaman Siber

Berdasarkan keseluruhan temuan, kesiapan nasional Indonesia dalam menghadapi ancaman siber masih berada pada tahap berkembang (developing stage). Indonesia telah memiliki struktur kebijakan dan kerangka regulasi yang cukup kuat, namun implementasi teknis dan koordinatif masih menjadi tantangan terbesar (Hidayat & Radyawanto, 2025). Beberapa aspek yang perlu diperkuat antara lain:

- Integrasi sistem keamanan lintas lembaga
- Deteksi ancaman berbasis kecerdasan buatan
- Peningkatan kapasitas SDM melalui sertifikasi professional
- Penguatan pusat data nasional dengan standar tier yang lebih tinggi
- Penyusunan protokol respons nasional terpadu untuk insiden berskala besar.

Penguatan keamanan siber Indonesia membutuhkan pendekatan yang tidak hanya berfokus pada aspek teknis, tetapi juga memperhatikan kesiapan kelembagaan dan budaya keamanan digital di seluruh sektor pemerintahan. Selain itu, hasil kajian juga menunjukkan bahwa adaptasi terhadap ancaman siber global harus dilakukan secara berkelanjutan, karena pola serangan kini semakin canggih, terdistribusi, dan memanfaatkan kecerdasan buatan untuk menembus sistem yang rentan. (Bhakti, Sudirman & Sumadinata (2024). Dengan meningkatnya ketergantungan pada layanan digital nasional, urgensi untuk membangun ekosistem keamanan siber yang terintegrasi menjadi semakin penting. Pemerintah perlu mempercepat harmonisasi kebijakan lintas sektor, memperkuat kapasitas analisis ancaman secara prediktif, serta memastikan adanya standardized incident response yang dapat diterapkan di seluruh level pemerintahan. Selain itu, kolaborasi antara pemerintah, industri teknologi, akademisi, dan komunitas keamanan siber harus terus diperluas untuk menciptakan ekosistem pertahanan siber yang adaptif. Literasi publik mengenai keamanan digital juga harus menjadi agenda prioritas nasional, mengingat tingginya kontribusi human error dalam berbagai insiden kebocoran data. (Ginting, Arifyanto & Ghafur (2023)

Dengan komitmen yang konsisten, peningkatan kapasitas SDM yang berkelanjutan, serta tata kelola digital yang terkoordinasi, Indonesia berpotensi mencapai tingkat ketahanan siber yang lebih kuat dan resilien. Hal ini menjadi fondasi penting dalam menjaga stabilitas layanan publik, kepercayaan masyarakat, serta keamanan nasional di tengah dinamika ancaman siber global yang terus berkembang. Selain itu, dinamika ancaman siber global menunjukkan bahwa Indonesia tidak hanya menghadapi serangan yang bersifat oportunistik, tetapi juga berpotensi menjadi target serangan yang lebih terstruktur dan berorientasi geopolitik (Bhakti, Sudirman, & Sumadinata, 2024). Sejumlah penelitian menunjukkan bahwa aktor negara (state-sponsored attackers) semakin aktif menyasar negara berkembang yang sedang mempercepat transformasi digital, termasuk Indonesia. Motifnya pun beragam, mulai dari pencurian data strategis, spionase digital, manipulasi sistem pelayanan publik, hingga upaya melemahkan stabilitas politik dan ekonomi. Kondisi ini menuntut Indonesia untuk memiliki kemampuan pertahanan siber yang tidak

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 13 Nomor 2 Februari 2026

hanya reaktif, tetapi juga proaktif melalui deteksi ancaman berbasis intelijen siber yang komprehensif (Ginting, Arifyanto, & Ghafur, 2023).

Di sisi lain, ketergantungan yang tinggi terhadap teknologi impor, baik perangkat keras maupun perangkat lunak, juga memperbesar risiko keamanan. Ketika infrastruktur digital nasional masih bergantung pada vendor luar negeri, potensi terjadinya supply chain attack semakin meningkat (Hidayat & Radyawanto, 2025). Kasus global seperti serangan terhadap SolarWinds menjadi contoh bagaimana celah keamanan pada rantai pasok digital dapat digunakan untuk menyusup ke berbagai instansi pemerintah sekaligus. Oleh karena itu, pengembangan kapasitas industri keamanan siber dalam negeri menjadi krusial agar Indonesia tidak hanya menjadi konsumen teknologi, tetapi juga mampu menciptakan solusi keamanan yang sesuai dengan karakteristik ekosistem digital nasional (Putri, Pratama, & Fithri, 2023).

Hasil kajian juga memperlihatkan bahwa pembangunan budaya keamanan siber (cybersecurity culture) merupakan aspek yang sering terabaikan tetapi memiliki pengaruh besar terhadap efektivitas pertahanan. Banyak insiden besar yang sejatinya dapat dicegah apabila ada disiplin penggunaan kata sandi, verifikasi dua langkah, prosedur akses terbatas, serta kebiasaan pelaporan dini terhadap aktivitas mencurigakan (Ginting et al., 2023). Peningkatan budaya keamanan tidak hanya penting bagi aparatur negara, tetapi juga bagi masyarakat luas yang menggunakan layanan digital pemerintah. Tanpa budaya keamanan yang kuat, investasi teknologi canggih sekalipun tidak akan memberikan hasil optimal (Rizki & Gustarina, 2024). Selain itu, ketimpangan kemampuan teknis antarinstansi pemerintah masih menjadi tantangan besar. Instansi pusat umumnya memiliki sistem yang lebih matang dan pendanaan yang lebih kuat dibandingkan pemerintah daerah (Padjadjaran University & Yani, 2024). Ketimpangan ini menciptakan celah besar dalam pertahanan nasional karena serangan siber hanya membutuhkan satu titik lemah untuk menembus sistem yang lebih besar. Untuk itu, standarisasi keamanan lintas daerah perlu mendapat perhatian khusus, termasuk penyediaan platform keamanan terpusat yang dapat digunakan oleh daerah dengan kapasitas teknis terbatas (Bhakti et al., 2024).

Dari perspektif kebijakan, harmonisasi regulasi juga menjadi kebutuhan mendesak. Meskipun berbagai peraturan telah diterbitkan, seperti kebijakan SPBE, perlindungan data pribadi, dan pedoman keamanan informasi, implementasinya sering berjalan secara parsial. Banyak instansi masih menggunakan standar internal masing-masing sehingga sulit menciptakan national cybersecurity posture yang benar-benar terpadu. Penyusunan protokol respons insiden nasional yang bersifat mengikat dan mengharuskan pelaporan real-time menjadi langkah penting untuk mengurangi kebingungan saat terjadi insiden besar seperti kasus PDNS (Hartati & Muhammad, 2024). Akhirnya, hasil analisis secara keseluruhan menunjukkan bahwa ketahanan siber Indonesia berada pada persimpangan penting. Di satu sisi, Indonesia memiliki potensi besar untuk memperkuat posisinya melalui inovasi digital, penguatan SDM, dan kerja sama strategis. (Hidayat & Radyawanto, 2025). Namun di sisi lain, celah keamanan yang belum tertutup secara menyeluruh dapat menjadi titik kritis apabila tidak segera ditangani melalui pendekatan yang komprehensif dan berkelanjutan. Dengan konsistensi kebijakan, peningkatan literasi dan budaya keamanan, serta akselerasi pembangunan infrastruktur digital yang aman, Indonesia dapat membangun fondasi pertahanan siber yang lebih resilien di masa depan. (Rizki & Gustarina, 2024).

KESIMPULAN

Berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa tantangan utama dalam memperkuat *cyber defense* terhadap infrastruktur digital pemerintah Indonesia terletak pada aspek sumber daya manusia, koordinasi antar lembaga, serta implementasi kebijakan keamanan siber yang belum sepenuhnya terintegrasi dengan sistem pemerintahan digital. Meningkatnya jumlah serangan siber hingga 3,64 miliar anomali pada tahun 2025 menegaskan bahwa digitalisasi yang pesat belum diimbangi dengan kesiapan pertahanan siber yang memadai. Kasus seperti serangan Ransomware LockBit 3.0 dan Brain Cipher menjadi bukti nyata kerentanan tersebut. Meskipun demikian, upaya pemerintah melalui

ISSN: 2406-8721 (Media Cetak) dan ISSN: 2406-8985 (Media Online)
Volume 13 Nomor 2 Februari 2026

pembentukan CSIRT, peningkatan kerja sama internasional, dan penerapan strategi *multi-layered defense* menunjukkan adanya langkah progresif menuju ketahanan siber nasional yang lebih tangguh. Untuk mencapai hal tersebut secara optimal, penguatan *cyber defense* tidak dapat hanya bergantung pada teknologi, melainkan juga menuntut tata kelola digital yang baik, peningkatan kesadaran keamanan siber, serta kolaborasi lintas sektor dan lembaga. Dengan pendekatan yang holistik dan berkelanjutan, Indonesia berpotensi membangun sistem pertahanan siber yang lebih resilien dan adaptif terhadap ancaman di era digital.

REFERENSI

Alfath, T. P., & Cahya, W. (2024). *Bridging the Gap Between Policy and Practice: Evaluating Indonesia's Ancaman Digital 2025: 133,4 Juta Serangan Siber Terjadi di RI*. (n.d.). CyberHub Indonesia.

Badan Siber dan Sandi Negara. (2024). *Laporan serangan siber 2024*.

Badan Siber dan Sandi Negara. (2025a). *Laporan anomali trafik serangan siber 2025*.

Bhakti, et al. (2024). Tantangan infrastruktur digital pemerintah. *Jurnal Keamanan Siber Nasional*.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, *9*(2), 27-40.

Cyber Threat Forecast 2025: Prediksi Ancaman Digital Global dan Dampaknya bagi Indonesia. (n.d.). Fourtrezz.

Cybersecurity Regulatory Framework (2020–2023). Data: Journal of Information Systems and Management, 2(1), 1–9.

De Nobrega, K. M. (2024). The whole of cyber defense: Syncing practice and theory. *Government Information Quarterly, 41*(2), Article 101893.

Ginting, et al. (2023). *Cyber hygiene dan human error*. *Jurnal Teknologi Pemerintahan*.

Hidayat, & Radyawanto. (2025). *Cybersecurity readiness index Indonesia*.

Hossain, S. T., Rahman, M., & Islam, M. S. (2025). Cybersecurity in local governments: A systematic review and future research agenda. *Government Information Quarterly, 42*(1), Article 101950.

Maharani, M. A. (2025). *Evaluasi Strategi Nasional Keamanan Siber Indonesia*. *Sosial Journal*, (terbit Juni 2025).

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative data analysis: A methods sourcebook. *(No Title)*.

Rexy, & Rexy. (2025, April 6). Cara Antisipasi Ancaman Siber 2025: Regulasi dan Solusinya di Indonesia - IT Proxsis Group. *IT Proxsis Group - Just another WordPress site*.

Rusydi, M. T. (2025). *Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats*. *Journal of Progressive Law and Legal Studies, 3*(1), 69–85.

Sulubara, et al. (2025). *Strategi CSIRT dan multi-layered defense*.

Syawaluddin, A. S. (2025). *Cyber Security dan Ketahanan Nasional*. *Jurnal Media Akademik*.

Team, D. (2025, April 21). Meningkatkan Keamanan Siber Nasional: Peran dan Tantangan di Tahun 2025. *DTrust*.