Konstitusi: Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi
Volume. 2, Nomor. 2 April 2025
e-ISSN: 3063-4040; p-ISSN: 3063-3877, Hal 257-266
DOI: https://doi.org/10.62383/konstitusi.v2i2.722
*Available Online at:*https://ejournal.appihi.or.id/index.php/Konstitusi

Analisis Strategi Keamanan Nasional Indonesia dalam Menghadapi Ancaman Siber

Galang Ramadhan
Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Indonesia

Alamat: Jl. Perintis Kemerdekaan No.KM.10, Tamalanrea Indah, Kec. Tamalanrea, Kota Makassar, SulawesiSelatan 90245
Korespondensipenulis: glgrmdhn0000@gmail.com

Abstract: *The rapid digital transformation has had a significant impact on various aspects of life, while simultaneously increasing the complexity of cyber threats faced by nations, including Indonesia. As a country with a high number of internet users, Indonesia is in a vulnerable position regarding cyberattacks that could threaten national stability. This study aims to analyze Indonesia's national security strategy in responding to cyber threats through a descriptive qualitative approach based on literature review and document analysis. The findings show that Indonesia has implemented various strategic policies, including the establishment of the National Cyber and Crypto Agency (BSSN), the enactment of regulations such as the Personal Data Protection Law, as well as the strengthening of international cooperation, human resource development, and the utilization of security technologies. However, significant challenges such as weak inter-agency coordination, low digital literacy, and limited infrastructure remain major obstacles to effective implementation. This study recommends strengthening governance, increasing institutional capacity, and involving multiple stakeholders to build a national cybersecurity system that is adaptive, inclusive, and sustainable.*

Keywords: *Technological Development, Cybersecurity, Indonesia, National Strategy, Digital Threats*

Abstrak: Transformasi digital yang pesat telah membawa dampak signifikan terhadap berbagai aspek kehidupan, namun sekaligus meningkatkan kompleksitas ancaman siber yang dihadapi oleh negara, termasuk Indonesia. Sebagai negara dengan jumlah pengguna internet yang tinggi, Indonesia berada dalam posisi rentan terhadap serangan siber yang dapat mengancam stabilitas nasional. Penelitian ini bertujuan untuk menganalisis strategi keamanan nasional Indonesia dalam merespons ancaman siber melalui pendekatan kualitatif deskriptif berbasis studi literatur dan analisis dokumen. Hasil kajian menunjukkan bahwa Indonesia telah mengimplementasikan berbagai kebijakan strategis, antara lain pembentukan Badan Siber dan Sandi Negara (BSSN), pengesahan regulasi seperti Undang-Undang Perlindungan Data Pribadi, serta penguatan kerja sama internasional, pengembangan sumber daya manusia, dan pemanfaatan teknologi keamanan. Namun, tantangan signifikan seperti lemahnya koordinasi antar lembaga, rendahnya literasi digital, serta keterbatasan infrastruktur masih menjadi hambatan utama dalam efektivitas pelaksanaannya. Studi ini merekomendasikan penguatan tata kelola, peningkatan kapasitas institusional, dan pelibatan multipihak guna membentuk sistem keamanan siber nasional yang adaptif, inklusif, dan berkelanjutan.

Kata kunci: PerkembanganTeknologi, Keamanan Siber, Indonesia, Strategi Nasional, Ancaman Digital

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi yang pesat di era digital telah membawa dampak signifikan terhadap berbagai sektor kehidupan manusia. Mulai dari ekonomi, pendidikan, kesehatan, hingga pemerintahan, perkembangan digital telah membawa berbagai kemudahan dan efesiensi terhadap semuanya. Namun, dibalik semua kemajuan tersebut, tentu ada ancaman terhadap dunia digital yang juga ikut berkembang pesat. Hal ini menimbulkan suatu tantangan baru yang semakin rumit dan terus berubah. (Kristianti, 2024).

Received: Maret 10, 2025; Revised: Maret 26, 2025; Accepted: April 23, 2025; Published: Juni 05, 2025

Indonesia, sebagai negara dengan jumlah penduduk terbanyak ke 4 di dunia, tentunya memiliki pengguna internet yang besar. Ini menjadikan Indonesia dalam posisi yang rentan akan ancaman keamanan siber. Keamanan siber menjadi semakin penting seiring dengan meningkatnya ketergantungan kita pada teknologi digital. Kebocoran data pribadi, serangan terhadap infrastruktur vital, serta penyebaran hoax melalui media digital menjadi contoh nyata dari ancaman siber yang semakin rumit. Hal ini dapat menyebabkan kerugian finasial, reputasi yang rusak, dan bahkan ancaman terhadap keamanan nasional.

Oleh karena itu, strategi keamanan nasional dalam menghadapi ancaman keamanan siber menjadi hal yang sangat penting untuk ditinjau, baik dari segi kebijakan, regulasi, maupun implementasi di lapangan. Tujuannya adalah untuk memastikan bahwa seluruh elemen negara, baik pemerintah, sektor swasta, maupun masyarakat umum, memiliki pemahaman yang sama serta kemampuan yang memadai dalam mendeteksi, mencegah, dan merespons setiap potensi serangan siber. Dengan hal tersebut diharapkan keamanan nasional dapat terjaga secara menyeluruh di era digital yang penuh tantangan ini.

Melalui tulisan ini, penulis ingin menganalisis bagaimana strategi keamanan nasional Indonesia dalam merespon ancaman keamanan siber, mengidentifikasi praktik terbaik, dan menganalisis tantangan yang akan dihadapi dalam implementasinya. Serta penulis berharap bahwa tulisan ini dapat memberikan wawasan dan rekomendasi yang berguna dan bermanfaat.

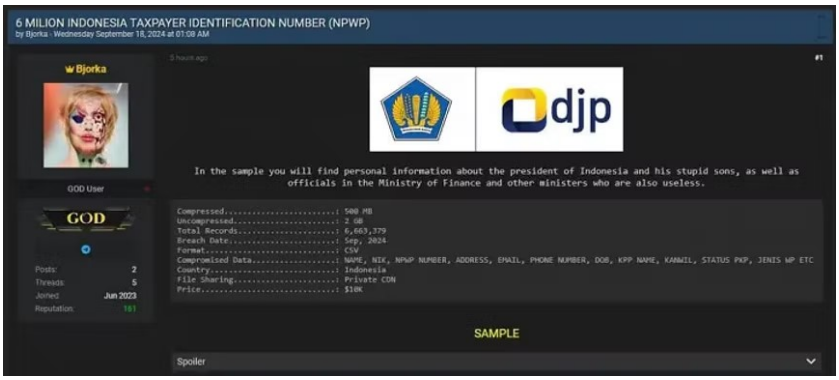
2. KAJIAN TEORITIS

Indonesia dan Ancaman Keamanan Siber

Perkembangan teknologi informasi telah membawa banyak perubahan besar dalam kehidupan masyarakat terkhususnya di Indonesia. Dengan bantuan teknologi informasi, komunikasi antar masyarakat menjadi lebih mudah dan cepat, tanpa mempedulikan keterbatasan waktu amupun jarak. Teknologi informasi juga memberikan konstribusi kepada negara dalam dua hal yang dianggap penting terhadap pertumbuhan suatu ekonomi. Pertama, meningkatnya kebutuhan akan produk-produk teknologi informasi, yang turut mendorong pertumbuhan industri terkait dan memacu inovasi serta pengembangan sektor tersebut. Lalu yang kedua, kemudahan yang ditawarkan kepada pelaku usaha, terutama dalam bidang keuangan dan bisnis. Melalui transformasi sistem pembayaran yang menjadi digital, munculnya e-commerce, serta layanan perbankan daring. Perubahan ini memungkinkan perusahaan beroperasi dengan lebih efisien dan efektif, serta membuka peluang ke pasar global (PB Oktaviani, 2021).

Namun, selain banyaknya manfaat yang diperoleh, berbarengan dengan itu juga muncul kerugiaan/ancaman dari perkembangan teknologi informasi ini. Indonesia sendiri termasuk dalam lima besar negara dengan tingkat penggunaan media sosial tertinggi, yang membawa dampak positif sekaligus potensi negatif, terutama dalam hal ancaman keamanan siber. Pemanfaatan teknologi digital di Indonesia memungkinkan terjadinya potensi ancaman keamanan siber yang dapat berdampak pada perang siber. Potensi yang dimaksud sebagai ancaman seperti peretasan, craking, sabotase dunia maya, dan perangkat mata-mata (Chintya Pradilla Putri, 2023). Beberapa kasus serangan siber yang terjadi di Indonesia seperti:

1. Kebocoran data ASN (2024)
2. Kasus pembobolan data NPWP Bjorka (2024)
3. Serangan Pusat Data Nasional Sementara, Ransomware Lockbit 3.0 (2024)
4. Kasus Peretasan Youtube DPR RI (2023)



Figur 1. Bjorka Menjual Data di Breach Forum pada Agustus, 2024

(Sumber: https://www.netmarks.co.id/post/serangan-siber-terbesar-yang-pernah-terjadi-di-indonesia)

Serangan siber ini membuat keamanan dan stabilitas ketertiban negara dapat terancam kapan saja. Selain menyebabkan kerugian yang sangat besar, kejadian diatas juga memberikan dampak jangka panjang, terutama pada reputasi dan kepercayaan masyarakat terhadap sebuah institusi atau pemerintah (Babys, 2021).

Secara singkat, pesatnya digitalisasi yang terjadi khususnya di Indonesia membawa dua sisi yang saling berlawanan layaknya uang koin. Pada satu sisi terdapat peluang efisiensi dan akselerasi pembangunan nasional, namun di sisi lainnya muncul ancaman keamanan siber yang semakin kompleks. Oleh karena itu, untuk merespons tantangan kejahatan siber, diperlukan kolaborasi lintas sektor, seperti pemerintah, penegak hukum, sektor swasta, serta masyarakat. Selain itu, penting untuk mengembangkan kerangka hukum yang fleksibel dan

menerapkan teknologi keamanan siber yang modern untuk mengatasi ancaman siber yang semakin banyak. (Eko Budi, 2021)

Strategi Indonesia

Dalam menghadapi ancaman keamanan siber, Indonesia telah mempunyai strategi keamanannya sendiri untuk menghadapi ancaman tersebut. Strategi keamanan nasional Indonesia dalam menghadapi ancaman keamanan siber telah dikembangkan dalam berbagai bentuk kebijakan, institusi, kerja sama internasional, serta peningkatan kapasitas sumber daya manusia dan teknologi.

Salah satu hasil penting yang dapat diidentifikasi adalah pembentukan Badan Siber dan Sandi Negara (BSSN), sebagai lembaga utama yang mengkoordinasikan dan melaksanakan kebijakan keamanan siber di Indonesia. BSSN bertanggung jawab atas koordinasi lintas sektor dalam pengelolaan insiden siber, pengembangan sistem keamanan digital nasional, serta penyusunan kebijakan dan pedoman teknis yang menjadi acuan bagi kementerian, lembaga, serta sektor swasta.

Figur 2. Lambang Badan Siber dan Sandi Negara (BSSN)
(Sumber: https://kompaspedia.kompas.id/baca/profil/lembaga/badan-siber-dan-sandi-negara-bssn)

Peran BSSN juga mencakup edukasi publik melalui kampanye kesadaran siber, penyediaan pelatihan teknis, hingga pelaksanaan audit keamanan pada instansi pemerintah dan lembaga vital. Dalam praktiknya, BSSN turut mengembangkan infrastruktur siber nasional yang tangguh, termasuk sistem pemantauan ancaman berbasis real-time dan pusat respons insiden siber nasional (*National Computer Security Incident Response Team* - ID-CERT). Lembaga ini menjadi garda depan dalam mencegah serta merespons serangan siber

yang mengancam kestabilan negara. Peran ini memperlihatkan bahwa BSSN memiliki kewenangan strategis yang sangat menentukan dalam menjaga integritas dan kedaulatan digital Indonesia, khususnya terhadap ancaman lintas batas dan spionase digital (Sihotang & Hoessein, 2025).

Secara regulatif, strategi keamanan nasional Indonesia telah diperkuat melalui sejumlah peraturan seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Regulasi ini bertujuan untuk memberikan kepastian hukum dan perlindungan terhadap data serta transaksi digital warga negara. Khusunya UU PDP yang menjadi tonggak penting dalam menjawab tantangan global mengenai privasi dan hak digital individu, terutama dalam konteks meningkatnya insiden kebocoran data. Selain itu, pemerintah juga telah menyusun Rencana Induk Keamanan Siber Nasional (RAN Kamsiberm) yang mencakup kebijakan teknis, strategi jangka panjang, serta mekanisme koordinasi antar lembaga. Namun, terdapat beberapa tantangan dalam harmonisasi kebijakan akibat tumpang tindih kewenangan, serta ketidaksinkronan antara kebijakan nasional dengan standar internasional. Maka dari itu, masih diperlukan konsistensi dan sinkronisasi lintas sektor untuk mendukung efektivitas strategi nasional ini, serta kebijakan strategis dalam keamanan siber harus terus diperbaharui secara adaptif agar mampu merespons dinamika ancaman siber yang berubah dengan cepat, baik dari dalam maupun luar negeri (Subroto, 2024).

Dalam konteks internasional, Indonesia telah menjalin kerja sama strategis dengan negara-negara mitra untuk memperkuat kapasitas teknis dan kelembagaan di bidang keamanan siber. salah satu contohnya adalah kerja sama Indonesia-Inggris yang terjalin dalam periode 2018–2028. Bentuk kerja sama ini meliputi pelatihan, transfer teknologi, serta penyusunan kebijakan bersama yang bertujuan membangun standar internasional dalam menangani ancaman siber. Kolaborasi semacam ini memberikan keuntungan dalam hal peningkatan keterampilan teknis dan pertukaran informasi intelijen siber, yang sangat dibutuhkan di tengah meningkatnya serangan digital global (Nurdiyanto et al, 2024).

Aspek lain yang juga tidak kalah penting adalah pembangunan kapasitas sumber daya manusia (SDM) di bidang keamanan siber. Tantangan utama dalam sektor ini adalah masih terbatasnya tenaga profesional yang kompeten, serta kurangnya kesadaran keamanan informasi di kalangan masyarakat luas. Oleh karena itu, berbagai program pelatihan, sertifikasi, dan pendidikan tinggi yang fokus pada keamanan siber mulai diterapkan. Pendekatan *digital forensic readiness* dapat digunakan sebagai salah satu strategi preventif

yang memungkinkan instansi pemerintah maupun swasta untuk lebih siap dalam menghadapi potensi serangan digital dengan respons yang sistematis (Widiyasono, 2024).

Penguatan teknologi dan infrastruktur juga menjadi bagian integral dari strategi nasional. Contohnya seperti implementasi sistem *honeypot* berbasis otomatisasi yang digunakan untuk mendeteksi dan menganalisis aktivitas siber yang mencurigakan secara real-time. Pemanfaatan teknologi seperti kecerdasan buatan (AI) dan *machine learning* juga mulai dikembangkan untuk meningkatkan efektivitas sistem deteksi dini terhadap serangan siber. Hal ini menandai pergeseran pendekatan dari responsif ke preventif, dimana sistem dapat mengenali pola serangan sebelum dampaknya meluas ke infrastruktur vital negara (Kurniawan & Saputra, 2024).

Diluar itu semua, penting untuk dicatat bahwa keamanan siber bukan hanya tanggung jawab pemerintah. Peran serta sektor swasta serta masyarakat umum juga memegang kunci dalam menciptakan ketahanan digital nasional yang berkelanjutan. Dalam hal ini, konsep seperti *Public-Private Partnership* (PPP) menjadi pendekatan strategis yang efektif. Kerja sama ini memungkinkan integrasi sistem manajemen keamanan informasi (ISMS) lintas sektor serta menciptakan mekanisme tanggap darurat yang efisien dan terkoordinasi (Firmansyah, 2024).

Secara keseluruhan, dapat dilihat bahwa strategi keamanan nasional Indonesia dalam menghadapi ancaman siber sudah mulai bergerak ke arah yang lebih terstruktur dan komprehensif. Keterlibatan berbagai aktor dari sektor publik, swasta, hingga akademisi menunjukkan sinergi nasional dalam mengatasi tantangan digital. Namun, keberhasilan implementasi strategi ini sangat bergantung pada keberlanjutan dukungan politik, alokasi sumber daya yang memadai, dan adopsi teknologi yang tepat guna. Oleh karena itu, strategi keamanan siber nasional harus terus diperbarui secara dinamis dan inklusif sesuai dengan perkembangan teknologi dan pola ancaman global.

3. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan fokus pada analisis berbagai literatur yang telah dipublikasikan *(publish)* di jurnal nasional maupun internasional. Penelitian ini bersifat deskriptif, bertujuan untuk menggambarkan makna dan esensi dari perang siber, serta mengidentifikasi solusi yang dapat diterapkan Indonesia dalam merespon isu tersebut. Untuk pengumpulan data, peneliti menerapkan metode analisis dokumen. Informasi diperoleh dari beragam sumber yang relevan, seperti laporan keamanan siber, studi kasus, dan artikel penelitian yang membahas ancaman serta penanganan keamanan siber. Data yang diperoleh

dianalisis untuk memberikan pemahaman mendalam mengenai karakteristik dan dampak dari ancaman siber, serta solusi yang telah diterpakan maupun yang masih dalam bentuk usulan untuk memperkuat keamanan digital. Selanjutnya, data dianalisis secara tematis untuk mengidentifikasi pola, tema, atau solusi yang dapat diterapkan. Diharapkan penelitian ini dapat menghilangkan kebingungan dalam memahami konsep perang siber dan memberikan wawasan lebih mandalam bagi berbagai pihak mengenai potensi ancaman dan tantangan yang ditimbulkannya, sekaligus pemikiran alternatif yang dapat dijadikan sebagai solusi khsususnya bagi Indonesia.

4. HASIL DAN PEMBAHASAN

Ancaman siber di era digital bukan hanya sekadar isu teknis, melainkan sudah menjadi tantangan strategis terhadap stabilitas nasional. Berdasarkan pembahasan sebelumnya, dapat dianalisis bahwa upaya pemerintah Indonesia melalui berbagai kebijakan dan kelembagaan memang menunjukkan keseriusan dalam membentuk sistem pertahanan siber nasional. Namun, meskipun berbagai langkah strategis telah diambil, implementasi di lapangan masih menghadapi sejumlah hambatan. Salah satu kelemahan utamanya adalah kurangnya koordinasi yang terpadu antar lembaga pemerintah. Di samping itu, keterbatasan anggaran serta rendahnya literasi digital di berbagai wilayah turut meningkatkan potensi terjadinya serangan siber berskala internasional. Serta upaya membangun budaya keamanan digital yang kuat di masyarakat masih belum sepenuhnya terbentuk. Maka perlu untuk dianalisis efektivitas dari strategi sebelumnya, agar diperoleh pemahaman yang lebih mendalam terhadap kekuatan, kelemahan, serta peluang dan ancaman yang dapat terjadi (Lubis et al, 2023).

Dari segi penguatan ketahanan siber nasional, pembentukan Badan Siber dan Sandi Negara (BSSN) dapat dianalisis sebagai bagian dari implementasi pendekatan *comprehensive national security* yang menyatukan unsur teknis, politik, dan sosial. BSSN bukan sekadar institusi teknokratis, melainkan aktor utama dalam ekosistem keamanan nasional yang berfungsi sebagai *central cyber authority*. Namun, efektivitas koordinatif lembaga ini masih dipengaruhi oleh tumpang tindih fungsi antar lembaga, khususnya dengan TNI, Polri, dan Kemenkominfo. Ketidakjelasan garis komando dan distribusi tanggung jawab antara lembaga-lembaga negara justru berpotensi menghambat kecepatan respons terhadap insiden siber skala nasional (Sihotang & Hoessein, 2025).

Lebih lanjut, dari sudut pandang *governance*, strategi legislasi seperti PP No. 71/2019 dan UU Perlindungan Data Pribadi (UU PDP) merupakan upaya penting untuk menciptakan

regulatory resilience. Namun regulasi tersebut menghadapi tantangan dalam proses implementasi di lapangan. Pelaksanaan UU PDP sering kali tidak diiringi dengan kesiapan institusional yang memadai, khususnya dalam hal infrastruktur pengawasan dan literasi hukum pelaku usaha digital. Akibatnya, keberadaan regulasi cenderung bersifat reaktif terhadap insiden, bukan bersifat preventif. Hal ini memperlihatkan bahwa regulasi yang baik tidak cukup hanya ditetapkan, namun juga harus didukung oleh perangkat pelaksana yang kuat dan sumber daya manusia yang memahami substansi serta urgensinya (Subroto, 2024).

Dalam perspektif teori *cyber deterrence*, strategi Indonesia cenderung masih bersifat defensif dibandingkan proaktif. Ini terlihat dari belum adanya doktrin pertahanan siber nasional yang secara jelas menggambarkan sikap dan strategi digital Indonesia terhadap potensi serangan lintas negara. Sementara itu, negara-negara seperti Amerika Serikat, Inggris, dan Tiongkok telah mengembangkan *cyber military doctrine* sebagai bentuk perlindungan atas kedaulatan digital. Dengan demikian, Indonesia perlu mempertimbangkan langkah yang lebih strategis dan diplomatis dalam merespons ancaman siber, termasuk membangun sistem diplomasi siber serta keterlibatan dalam perjanjian multilateral mengenai tata kelola internet dan keamanan digital.

Lalu, juga ditekankan bahwa keberhasilan strategi keamanan siber tidak dapat dilepaskan dari keterlibatan berbagai pihak. Keterlibatan sektor swasta dan masyarakat sipil sangat penting dalam membentuk budaya sadar siber. Model *Public-Private Partnership* (PPP) dinilai relevan untuk mendorong kolaborasi antara pemerintah dan sektor non-negara dalam membangun ekosistem keamanan siber yang adaptif dan inklusif. Namun, pendekatan ini masih terkendala oleh ketimpangan akses teknologi, dominasi perusahaan asing dalam sistem keamanan, serta kurangnya standar interoperabilitas antar platform digital yang digunakan oleh berbagai lembaga di Indonesia (Firmansyah, 2024).

Melalui analisis *SWOT* terhadap kondisi keamanan siber nasional, terlihat bahwa adanya kekuatan pada sisi regulasi dan kelembagaan, tetapi masih lemah pada hal koordinasi dan kesiapan operasional. Terdapat peluang besar melalui kerja sama internasional, investasi teknologi, dan peningkatan SDM. Namun, disisi lain terdapat ancaman seperti serangan siber didukung negara, kebocoran data skala besar, dan perang informasi menjadi faktor eksternal yang perlu diwaspadai. Dengan demikian, jelas bahwa strategi keamanan nasional di ruang digital harus bersifat sistemik dan mampu beradaptasi. Indonesia harus segera memperkuat tata kelola, meningkatkan kolaborasi antar aktor, dan membangun kapasitas masyarakat guna menciptakan ketahanan siber nasional yang tangguh dan berkelanjutan.

5. KESIMPULAN DAN SARAN

Berdasarkan pembahasan di atas, dapat disimpulkan bahwa Indonesia menghadapi tantangan besar dalam menjaga keamanan siber di tengah pesatnya perkembangan teknologi informasi. Perkembangan ini membawa manfaat dan dampak positif, namun juga terdapat ancaman dan resiko yang lebih kompleks. Pemerintah sendiri telah membuat strategi untuk menghadapinya, seperti pembentukan BSSN, menyusun regulasi seperti UU PDP, memperkuat kerja sama internasional, mengembangkan SDM serta teknologi keamanan. Akan tetapi efektivitas implementasinya masih terkendala oleh lemahnya koordinasi antar lembaga, rendahnya literasi digital, dan minimnya kesiapan institusional. Oleh karena itu, diperlukan strategi keamanan siber yang lebih sistemik, adaptif, dan inklusif,sertaperluadanyapeningkataninvestasi di bidangriset dan teknologikeamanansiber, dan pelibatanaktifsektorwisatamaupunmasyarakat. Itu semuadibutuhkanuntuk membangun ketahanan siber nasional yang berkelanjutan dan tangguh terhadap dinamika ancaman globalsertamenciptakanekosistem digital yang aman dan terpercaya.

DAFTAR REFERENSI

Jurnal:

Babys, S. A. M. (2021). Ancaman perang siber di era digital dan solusi keamanan Indonesia. *Jurnal Oratio Directa*, *3*(1), 425–442. https://ejurnal.ubk.ac.id/index.php/oratio/article/view/163

Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Firmansyah, R. A. (2024). *Framework integrasi digital forensic readiness dan information security management system di lingkungan pemerintahan* [Skripsi, Universitas Islam Indonesia].

Handoko, G. R. (2020). *Optimalisasi manajemen media informasi di era digital untuk ketahanan nasional*. Lembaga Ketahanan Nasional Republik Indonesia.

Kristianti, N., & Ririn, K. (2024). Peraturan dan regulasi keamanan siber di era digital. *Satya Dharma: Jurnal Ilmu Hukum*, *6055*(1), 297–310. https://ejournal.iahntp.ac.id/index.php/satya-dhamat

Kurniawan, D., & Yuliana, M. S. (2024). Implementasi Ansible pada otomasi honeypot deployment berbasis web. *Journal of Internet and Software Engineering*, *5*(2), 86–98.

Lubis, A. J., Cempaka, F. G., & Siahaan, S. (2023). Perang cyber sebagai bentuk peperangan asimetris: Perspektif filsafat keamanan digital dan NIST Cybersecurity Framework. *Jurnal Ilmu Pengetahuan Sosial*, *10*(10), 4607–4617.

Nurdiyanto, R. A., Subagyo, A., & Sari, S. (2024). Kerjasama keamanan siber Indonesia–Inggris pada periode 2018–2028. *Jurnal Mahasiswa Magister Hubungan Internasional*, *1*(1), 339–349. https://doi.org/10.36859/dgsj.v1i1.2889

Oktaviani, P. B., & Silvia, A. (2021). Strategi keamanan siber Malaysia. *Jurnal Kajian Ilmiah*, *21*(1), 69–84. https://doi.org/10.31599/jki.v21i1.447

Putri, C. P., Anggraini, W., Hasibuan, Y. M., & Nurbaiti, N. (2023). Strategi pengamanan cyber: Lingkup kerjasama dalam menghadapi ancaman cyber. *INSOLOGI: Jurnal Sains dan Teknologi*, *2*(6), 1124–1130. https://doi.org/10.55123/insologi.v2i6.2847

Sihotang, M., & Hoessein, Z. A. (2025). Transformasi politik hukum dalam penguatan regulasi cyber law di Indonesia. *Jurnal Hukum dan Teknologi Digital*, *6*(1). *(Catatan: Tambahkan nama jurnal lengkap jika tersedia)*

Subroto, M. I. (2024). Perkembangan kerja sama pertahanan Indonesia. *Jurnal Mahasiswa Magister Hubungan Internasional*, *1*(1), 610–634. https://doi.org/10.36859/dgsj.v1i1.2906

Widiyasono, N. (2024). *Pengantar forensika digital* (Edisi Desember 2024). CV Angkasa Media Literasi.

Website:

Aldiansyah, F. (2025, 11 Februari). *Serangan siber terbesar yang pernah terjadi di Indonesia*. Netmarks Indonesia. https://www.netmarks.co.id/post/serangan-siber-terbesar-yang-pernah-terjadi-di-indonesia

Chryshna, M. (2021, 4 Juli). *Lembaga Siber dan Sandi Negara (BSSN)*. Kompas Pedia. https://kompaspedia.kompas.id/baca/profil/lembaga/badan-siber-dan-sandi-negara-bssn

Cloudeka. (2023, 26 Juli). *10 contoh kasus cyber crime yang bisa menjadi pelajaran*. Lintasarta Cloudeka. https://www.cloudeka.id/id/berita/web-sec/contoh-kasus-cyber-crime/

Sugiarti, U. (2024, 9 September). *10 kasus hacking paling menggemparkan di Indonesia*. Lawencon. https://www.lawencon.com/daftar-kasus-hacking-di-indonesia/