

PERLINDUNGAN DATA DAN INFRASTRUKTUR DIGITAL DALAM KONTEKS CYBER WARFARE:
TINJAUAN HUKUM TEKNOLOGI INFORMASIAidan Rafif¹Email: 2210611338@mahasiswa.upnvj.ac.id

Fakultas Hukum, Universitas Pembangunan Nasional “Veteran” Jakarta

Abstract

The rapid advancement of information technology has positioned data and digital infrastructure as fundamental components of national stability and resilience. At the same time, the growing escalation of cyberattacks particularly the most critical form known as cyber warfare poses significant challenges to Indonesia's efforts in safeguarding data and ensuring digital security. This study examines how Indonesia's national legal framework regulates data protection and digital infrastructure security, while also assessing the extent to which these regulations align with international legal principles and practices in addressing cross-border cyberattacks. This research employs a qualitative method with a normative juridical approach by analyzing legislation, official documents, academic literature, and relevant international legal instruments. The findings indicate that Indonesia has established a relatively solid regulatory basis, including the Electronic Information and Transactions Law (ITE Law), Government Regulation No. 71/2019, and the Personal Data Protection Law (PDP Law), complemented by technical guidelines issued by the National Cyber and Encryption Agency (BSSN). However, several challenges persist in practice, such as suboptimal inter-agency coordination, uneven cybersecurity standards across sectors, and limited state capacity in attributing cyberattacks. When compared to international principles such as those outlined in the Tallinn Manual and other global cybersecurity frameworks certain areas within Indonesia's regulations still require improvement. Overall, this study underscores the need for regulatory reform, harmonization of national standards with global frameworks, and greater institutional capacity-building to strengthen Indonesia's cyber defense posture amid the growing threats of cyber warfare.

Keywords: *Data protection, Cybersecurity, Cyber warfare.*

Article History

Received: Desember 2025
Reviewed: Desember 2025
Published: Desember 2025

Copyright : Author
Publish by : CAUSA



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

Abstrak

Kemajuan teknologi informasi telah menempatkan data dan infrastruktur digital sebagai elemen krusial bagi stabilitas dan ketahanan negara. Di sisi lain, meningkatnya eskalasi serangan siber, termasuk bentuk yang paling ekstrem yaitu cyber warfare, menghadirkan tantangan serius terhadap upaya perlindungan data dan keamanan digital di Indonesia. Penelitian ini berfokus untuk mengkaji bagaimana kerangka hukum nasional mengatur perlindungan data dan keamanan infrastruktur digital, serta menilai sejauh mana aturan tersebut telah selaras dengan prinsip dan praktik hukum internasional dalam menghadapi serangan siber lintas negara. Pendekatan penelitian menggunakan metode kualitatif dengan teknik yuridis normatif melalui analisis peraturan perundang-undangan, dokumen resmi, literatur akademik, serta instrumen hukum internasional. Hasil kajian menunjukkan bahwa Indonesia telah memiliki dasar hukum yang cukup kuat, seperti UU ITE, PP PSTE, dan UU PDP, disertai pedoman teknis dari BSSN. Namun demikian, penerapannya masih menemui sejumlah hambatan, antara lain koordinasi antarlembaga yang belum optimal, disparitas standar keamanan di berbagai sektor, serta keterbatasan dalam kemampuan melakukan atribusi serangan siber. Jika dibandingkan dengan prinsip internasional, seperti aturan yang diuraikan dalam Tallinn Manual dan standar keamanan global lainnya, masih terdapat beberapa aspek yang perlu diperkuat. Secara keseluruhan, penelitian ini menekankan perlunya pembaruan regulasi, harmonisasi standar nasional dengan kerangka global, serta penguatan kapasitas kelembagaan untuk membangun sistem pertahanan siber yang lebih tangguh di tengah ancaman cyber warfare yang terus berkembang.

Kata kunci: Perlindungan data, Keamanan siber, Cyber warfare

PENDAHULUAN

Perkembangan teknologi informasi dalam dua puluh tahun terakhir telah membawa perubahan besar dalam hampir semua aspek kehidupan manusia. Tidak hanya cara kita berkomunikasi dan berinteraksi, tetapi juga sistem ekonomi, layanan publik, serta tata kelola pemerintahan ikut terdampak oleh proses digitalisasi yang semakin cepat.¹ Dalam ekosistem

¹ Mukhsin, M. (2020). Peranan teknologi informasi dan komunikasi menerapkan sistem informasi desa dalam publikasi informasi desa di era globalisasi. Teknokom, 3(1), 7-15.

baru ini, data menjelma menjadi aset strategis yang memiliki nilai tinggi, sementara infrastruktur digital berfungsi sebagai penopang utama bagi berbagai aktivitas penting negara. Ketergantungan yang makin kuat terhadap teknologi informasi membuat isu keamanan data dan keandalan infrastruktur digital menjadi semakin vital untuk menjaga stabilitas nasional. Di tengah lajunya transformasi digital tersebut, muncul pula ancaman yang bersifat lebih kompleks dan berbahaya, yakni *cyber warfare* atau perang siber, yang kini menjadi perhatian serius dalam bidang keamanan internasional.²

Cyber warfare tidak lagi dipandang sebagai ancaman abstrak. Dalam kenyataannya, ia telah menjadi alat nyata yang digunakan dalam konflik antarnegara maupun oleh aktor non-negara. Serangan siber dapat dilakukan secara senyap, melampaui batas negara, dan menghasilkan dampak kerusakan yang dapat menyamai serangan fisik.³ Infrastruktur vital seperti jaringan listrik, transportasi, layanan kesehatan, data kependudukan, dan pusat data pemerintah menjadi sasaran empuk bagi kelompok peretas yang beroperasi dengan kemampuan teknis tinggi, baik yang berasal dari luar negeri maupun dalam negeri. Berbagai insiden di tingkat global menunjukkan bahwa serangan siber mampu melumpuhkan layanan publik, menyebabkan kebocoran data dalam skala besar, hingga menimbulkan kerugian ekonomi yang mencapai miliaran dolar. Fenomena ini memperlihatkan bahwa *cyber warfare* membawa dampak yang jauh lebih luas dibandingkan bentuk serangan digital biasa.⁴

Indonesia juga menghadapi situasi serupa. Transformasi digital yang berlangsung cepat ternyata tidak selalu diimbangi dengan kesiapan sistem keamanan informasi yang memadai. Serangan ransomware terhadap Pusat Data Nasional (PDN) pada tahun 2024 menjadi bukti nyata bahwa infrastruktur digital strategis Indonesia masih memiliki celah kerentanan yang serius. Di sisi lain, berbagai insiden kebocoran data masyarakat mulai dari data kesehatan, kependudukan, hingga data perbankan yang mengungkap lemahnya tata kelola perlindungan data dan kurangnya penerapan standar keamanan digital di berbagai instansi. Upaya peretasan terhadap lembaga pemerintah, telekomunikasi, dan platform digital nasional juga terus bermunculan, menandakan bahwa ancaman *cyber warfare* semakin menguat, terstruktur, dan sulit diprediksi.

Dalam kondisi tersebut, kehadiran regulasi menjadi sangat penting sebagai dasar perlindungan hukum sekaligus pedoman tata kelola keamanan siber yang lebih kuat. Indonesia

² Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Strategik Ketahanan Nasional*, 6(2), 5. Hlm 3

³ Arianto, A. (2025). *Cyber warfare dalam Konflik Modern: Analisis Serangan Stuxnet pada Fasilitas Nuklir Iran*. *Dialogika: Jurnal Penelitian Komunikasi dan Sosialisasi*, 1(3), 41-52.

⁴ Febriansyah, F. I., & SH, M. (2025). *Cybercrime: Kejahatan di Balik Layar Digital*. *Najaha*.hlm 10

telah memiliki sejumlah perangkat hukum, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), serta Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022.⁵ Semua regulasi ini menunjukkan upaya negara untuk merespons tantangan digital yang semakin kompleks. Namun pertanyaan penting tetap muncul: apakah kerangka hukum tersebut sudah cukup untuk menghadapi ancaman *cyber warfare* yang berkembang cepat dan melibatkan aktor dengan kemampuan teknis yang sangat tinggi. Tantangan implementasi juga menjadi persoalan besar. Koordinasi antar lembaga keamanan siber sering kali belum berjalan efektif, sehingga penanganan insiden siber tidak selalu cepat dan terkoordinasi. Standar keamanan yang digunakan oleh instansi pemerintah dan sektor swasta pun belum seragam, menciptakan kesenjangan antara kebutuhan dan kondisi aktual di lapangan.⁶ Sistem deteksi, mitigasi, dan pemulihan insiden siber juga belum sepenuhnya kuat untuk menahan serangan masif dan terorganisasi. Kondisi ini membuat infrastruktur digital strategis Indonesia berada dalam posisi yang rentan.

Dalam perspektif hukum teknologi informasi, perlindungan data dan keamanan infrastruktur digital tidak hanya dipandang sebagai persoalan teknis, tetapi juga menyangkut dimensi normatif, kelembagaan, dan kebijakan publik. Regulasi perlu memberikan kejelasan mengenai tanggung jawab berbagai pihak dalam pengelolaan data dan sistem elektronik, mekanisme penyelesaian sengketa, serta kewajiban pelaporan ketika terjadi insiden kebocoran atau serangan siber. Selain itu, hukum harus mampu mengantisipasi pola-pola baru dalam *cyber warfare*, termasuk serangan yang melibatkan negara asing atau kelompok siber internasional yang sulit dilacak.

Melihat kompleksitas ancaman tersebut, penelitian mengenai perlindungan data dan keamanan infrastruktur digital menjadi sangat penting. Penelitian ini bertujuan untuk menilai sejauh mana kerangka hukum Indonesia mampu memberikan perlindungan yang memadai terhadap data dan infrastruktur digital di tengah meningkatnya ancaman *cyber warfare*. Selain itu, analisis ini juga berusaha mengidentifikasi kelemahan regulasi, hambatan implementasi, serta kebutuhan reformasi hukum yang diperlukan untuk memperkuat ketahanan siber nasional. Dengan pemahaman yang lebih mendalam, diharapkan penelitian ini dapat memberikan

⁵ Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(2), 222-238.

⁶ Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 10(2), 113-128.

kontribusi terhadap penguatan perlindungan hukum di era perang siber yang semakin dinamis dan penuh risiko.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan yuridis normatif, yaitu pendekatan penelitian hukum yang berfokus pada kajian terhadap teks, norma, serta dokumen hukum sebagai sumber data utama. Pendekatan ini dipilih karena penelitian bertujuan memahami bagaimana kerangka hukum Indonesia mengatur perlindungan data dan keamanan infrastruktur digital dalam konteks ancaman *cyber warfare*, sekaligus menilai sejauh mana aturan nasional tersebut selaras dengan prinsip-prinsip hukum internasional.⁷ Melalui pendekatan normatif, penelitian dapat menelaah berbagai norma positif, asas hukum, dan kebijakan yang tertuang dalam peraturan perundang-undangan seperti UU ITE, PP 71 Tahun 2019, serta Undang-Undang Perlindungan Data Pribadi (UU PDP) dan juga serta mengkomparasikannya dengan instrumen global seperti *Tallinn Manual* dan standar keamanan siber internasional lainnya.

Sumber data penelitian terdiri atas bahan hukum primer, seperti undang-undang, peraturan pemerintah, putusan pengadilan, serta dokumen resmi dari lembaga yang berwenang mengelola keamanan siber, termasuk BSSN dan Kementerian Komunikasi dan Informatika. Penelitian ini juga memanfaatkan bahan hukum sekunder berupa buku, jurnal ilmiah nasional, karya ilmiah, serta publikasi akademik yang membahas isu perlindungan data, keamanan informasi, dan *cyber warfare*. Untuk memperkuat analisis, bahan hukum tersier seperti kamus hukum, ensiklopedia, dan indeks regulasi juga digunakan.

Pengumpulan data dilakukan melalui studi pustaka (*library research*) dengan menelusuri literatur hukum, artikel ilmiah, serta dokumen pemerintah yang relevan dan terpercaya. Seluruh data yang diperoleh dianalisis menggunakan teknik analisis kualitatif, yaitu dengan mengidentifikasi, menguraikan, dan menginterpretasikan berbagai aturan hukum serta literatur yang ada.⁸ Proses analisis dilakukan secara sistematis untuk membandingkan ketentuan hukum Indonesia dengan standar internasional, sekaligus mengungkap kesenjangan regulasi (*gap analysis*) dan hambatan implementasi yang masih terjadi. Dengan pendekatan ini, penelitian diharapkan mampu memberikan gambaran yang lebih menyeluruh mengenai efektivitas kerangka hukum nasional dalam menghadapi ancaman *cyber warfare* serta mengidentifikasi

⁷ Rukin, S. P. (2019). Metodologi penelitian kualitatif. Yayasan Ahmar Cendekia Indonesia.

⁸ Tahir, R., Astawa, I. G. P., Widjajanto, A., Panggabean, M. L., Rohman, M. M., Dewi, N. P. P., ... & Paminto, S. R. (2023). Metodologi penelitian bidang hukum: Suatu pendekatan teori dan praktik. PT. Sonpedia Publishing Indonesia.

kebutuhan pembaruan regulasi guna memperkuat perlindungan data dan ketahanan infrastruktur digital Indonesia.

PEMBAHASAN

A. kerangka hukum Indonesia mengatur perlindungan data dan keamanan infrastruktur digital dalam menghadapi ancaman *cyber warfare*

Kerangka hukum Indonesia dalam melindungi data dan mengamankan infrastruktur digital pada dasarnya dibentuk melalui serangkaian regulasi yang dirancang untuk memperkuat tata kelola keamanan siber, terutama dalam menghadapi ancaman modern seperti *cyber warfare*. Salah satu fondasi awalnya adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang menjadi pijakan formal bagi aturan penyelenggaraan sistem elektronik serta keamanan informasi di Indonesia. Melalui UU ITE dan perubahan-perubahannya, pemerintah mewajibkan setiap penyelenggara sistem elektronik (PSE) menjaga keamanan sistem dan melindungi data pribadi para penggunanya.⁹ Meski demikian, efektivitas aturan tersebut sering dipertanyakan, terutama ketika dihadapkan pada serangan siber besar yang terorganisasi dan melibatkan aktor dengan kemampuan teknis tinggi, termasuk serangan yang bersifat lintas negara.

Dapat dikatakan lebih rinci Kerangka hukum Indonesia dalam melindungi data dan mengamankan infrastruktur digital dibangun melalui sejumlah regulasi yang dirancang untuk memperkuat tata kelola keamanan siber nasional. Upaya ini semakin relevan mengingat serangan siber yang bersifat terstruktur, lintas negara, dan terkait potensi *cyber warfare* semakin meningkat. Salah satu pondasi utamanya adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang pertama kali disahkan melalui UU No. 11 Tahun 2008 dan kemudian diperbarui melalui UU No. 19 Tahun 2016. UU ITE mengatur sejumlah kewajiban penyelenggara sistem elektronik (PSE) terkait perlindungan data dan keamanan sistem. Misalnya, Pasal 15 UU ITE menegaskan bahwa PSE wajib memberikan “perlindungan yang sepatutnya terhadap keamanan informasi, sistem, dan sarana yang digunakan dalam penyelenggaraan sistem elektronik.” Ini berarti PSE memiliki tanggung jawab hukum untuk menjaga keamanan sistem dari akses tidak sah, gangguan operasional, hingga kebocoran data.

⁹ Idris, J. I., & Supandi, A. (2024). Evaluasi Kebijakan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia; Potret Bibliometric Analysis. *Transparansi: Jurnal Ilmiah Ilmu Administrasi*, 7(1), 149-162.

Namun, efektivitas ketentuan tersebut tetap menjadi perdebatan, terutama ketika Indonesia dihadapkan pada serangan siber berskala besar yang melibatkan aktor negara maupun non-negara.

Penerapan lebih teknis dari UU ITE kemudian diperjelas melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). PP ini memberikan batasan dan tanggung jawab hukum yang lebih spesifik, terutama dalam Pasal 20-25, yang mewajibkan PSE menerapkan prinsip-prinsip keamanan informasi seperti kerahasiaan (*confidentiality*), integritas (*integrity*), keaslian (*authenticity*), dan ketersediaan (*availability*).¹⁰ Selain itu, Pasal 28-29 PP PSTE mewajibkan PSE melakukan audit keamanan sistem secara berkala, menyediakan prosedur manajemen insiden, serta melaporkan setiap insiden keamanan kepada pihak berwenang, yaitu BSSN atau kementerian terkait. Dalam konteks ancaman cyber warfare, pasal-pasal ini menjadi dasar penting karena mewajibkan standar pertahanan digital yang lebih tinggi bagi PSE yang mengelola sektor strategis, seperti pusat data pemerintah, sektor energi, kesehatan, dan keuangan.

Langkah signifikan berikutnya datang melalui disahkannya Undang-Undang Perlindungan Data Pribadi (UU PDP) Nomor 27 Tahun 2022, yang menjadi tonggak besar dalam sistem perlindungan data Indonesia. UU PDP memberikan kewajiban lebih tegas bagi pengendali data (*data controller*) dan pemroses data (*data processor*). Pasal 39-40 UU PDP mewajibkan setiap pengendali data untuk menerapkan langkah keamanan elektronik dan non-elektronik guna melindungi data pribadi dari akses ilegal, peretasan, manipulasi, atau kebocoran.¹¹ Selain itu, Pasal 46 UU PDP mengatur kewajiban pengendali data untuk memberitahu subjek data dan otoritas terkait jika terjadi kebocoran data dalam jangka waktu paling lambat 3 x 24 jam sejak insiden terdeteksi. Ketentuan ini menjadi sangat penting dalam konteks cyber warfare, di mana serangan sering kali menasar data pribadi skala besar untuk kepentingan spionase, sabotase, atau destabilisasi publik.

Selain perangkat regulasi, peran Badan Siber dan Sandi Negara (BSSN) juga sangat penting dalam membangun ekosistem keamanan digital nasional. BSSN telah merumuskan sejumlah pedoman teknis, termasuk Indeks Keamanan Informasi (KAMI) dan pedoman manajemen risiko siber, yang ditujukan untuk membantu institusi pemerintah maupun swasta meningkatkan sistem pertahanannya.¹² Namun, temuan berbagai penelitian menyoroiti bahwa adopsi pedoman

¹⁰ Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). Keamanan Data dan Informasi. Kaizen Media Publishing. Hlm 18

¹¹ Budiandru, B., & Hidayat, R. S. (2025). Tanggung Jawab Hukum Marketplace terhadap Kebocoran Data Pribadi Pengguna dalam Perspektif UU ITE dan UU Perlindungan Data Pribadi. RIGGS: Journal of Artificial Intelligence and Digital Business, 4(3), 7738-7743.

¹² Ginanjar, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. Dinamika Global: Jurnal Ilmu Hubungan Internasional, 7(02), 295-316.

tersebut belum merata. Banyak instansi, terutama di daerah atau sektor swasta yang memiliki keterbatasan sumber daya, belum mampu menerapkannya secara optimal.⁵ Kondisi ini turut menjelaskan mengapa kasus kebocoran data dan serangan siber yang berhasil masih kerap terjadi di Indonesia.

Insiden *ransomware* yang menyerang Pusat Data Nasional (PDN) pada tahun 2024 menjadi contoh nyata bahwa penerapan kerangka hukum yang sudah ada belum sepenuhnya efektif. Serangan tersebut memperlihatkan adanya jurang antara aturan hukum dan praktik keamanan di lapangan, seperti kurangnya audit keamanan berkala, lemahnya sistem cadangan data, serta tidak adanya koordinasi yang cepat dan terarah antar lembaga saat insiden terjadi.¹³ Peristiwa ini menegaskan bahwa meskipun regulasi keamanan siber Indonesia telah tersusun cukup lengkap, penerapannya masih menghadapi banyak tantangan, terutama ketika berhadapan dengan ancaman *cyber warfare* yang sifatnya kompleks dan terorganisasi.

B. Sejauh mana regulasi nasional selaras dengan prinsip dan praktik internasional dalam menangani serangan siber yang bersifat lintas negara

Dalam konteks internasional, serangan siber yang melintasi batas negara kini semakin sering terjadi dan menuntut adanya aturan hukum nasional yang selaras dengan prinsip global. Indonesia, sebagai bagian dari komunitas dunia, berkepentingan untuk menyesuaikan kerangka hukumnya dengan standar keamanan siber internasional, terutama dalam menghadapi bentuk ancaman baru seperti *cyber warfare*. Sejumlah regulasi nasional seperti UU ITE, PP PSTE, dan UU PDP yang sebenarnya sudah memuat berbagai prinsip dasar yang juga dianut secara global, misalnya terkait perlindungan kerahasiaan data, keamanan penyelenggara sistem elektronik, dan kewajiban melindungi data pribadi.

Meski demikian, bila dibandingkan dengan pedoman internasional seperti *Tallinn Manual 2.0*, yang selama ini menjadi rujukan utama dalam hukum internasional berkaitan dengan operasi siber dan *cyber warfare*, masih terdapat sejumlah celah. *Tallinn Manual* menegaskan pentingnya kejelasan mengenai atribusi serangan, prinsip kehati-hatian negara, kewajiban *due diligence*, serta aturan mengenai batas penggunaan kekuatan dalam konflik siber.¹⁴ Sementara itu, pengaturan di Indonesia belum secara tegas mengatur isu atribusi ataupun peran negara dalam serangan siber, padahal aspek ini merupakan salah satu isu paling

¹³ KOTA, M. K. S. D. I. LEMBAGA KETAHANAN NASIONAL REPUBLIK INDONESIA. Hlm 5

¹⁴ Gunawan, R., Simangunsong, R., Susilo, T., Limbong, B., & Soeprianto, A. (2025). Penerapan Hukum Humaniter dalam Konflik Siber: Tantangan, Implikasi, dan Kebutuhan Standar Baru. JURNAL SYNTAX IMPERATIF: Jurnal Ilmu Sosial dan Pendidikan, 6(2), 165-173.

krusial karena serangan biasanya dilakukan dengan cara yang sulit dilacak baik secara teknis maupun politis.

Selanjutnya, standar praktik internasional seperti *NIST Cybersecurity Framework* serta pedoman keamanan dari *International Telecommunication Union* (ITU) juga belum sepenuhnya diintegrasikan dalam regulasi nasional.¹⁵ Berbagai riset menunjukkan bahwa Indonesia masih berada dalam proses membangun kerangka manajemen risiko siber yang setara dengan standar global, terutama dalam hal kemampuan deteksi dini dan penanggulangan serangan. Kurangnya pemahaman dan penerapan standar internasional pada banyak instansi pemerintah turut menimbulkan perbedaan tingkat keamanan siber antar sektor.

Dari sisi kerja sama lintas negara, Indonesia memang telah terlibat dalam beberapa forum, termasuk *ASEAN Cybersecurity Cooperation*, serta menjalin kerja sama bilateral dengan negara seperti Singapura dan Jepang. Tetapi sejumlah analisis menilai bahwa pola kerja sama tersebut masih cenderung bersifat responsif dan belum diarahkan pada pembangunan sistem pertahanan siber yang lebih terstruktur dan berkelanjutan.¹⁶ Dengan melihat kondisi tersebut, terlihat bahwa kerangka hukum nasional sudah memiliki fondasi yang cukup kuat, tetapi masih perlu diperkuat agar selaras dengan norma dan standar internasional. Diperlukan langkah strategis berupa pembaruan regulasi yang lebih adaptif, peningkatan kapabilitas atribusi serangan, harmonisasi standar keamanan nasional dengan kerangka global, serta penguatan kerja sama internasional yang lebih proaktif dan terarah.

KESIMPULAN

Perkembangan teknologi informasi telah membawa perubahan besar dalam cara negara mengelola data dan mengandalkan infrastruktur digital, sehingga kedua elemen tersebut kini menjadi komponen penting dalam penyelenggaraan layanan publik dan perlindungan keamanan nasional. Namun, meningkatnya intensitas serta kompleksitas ancaman siber terutama yang berkaitan dengan *cyber warfare* dalam menunjukkan bahwa Indonesia masih menghadapi berbagai kendala dalam menjaga keamanan aset digital yang bersifat strategis. Walaupun kerangka hukum nasional seperti UU ITE, PP PSTE, UU PDP, dan sejumlah pedoman teknis dari BSSN telah memberikan dasar yang cukup kuat, penerapannya di lapangan masih belum

¹⁵ Lubis, Ahmad Jufri, and Suhirwan Suhirwan. "PERANG CYBER SEBAGAI BENTUK PEPERANGAN ASIMETRIS: PERSPEKTIF FILSAFAT KEAMANAN DIGITAL DAN NIST CYBERSECURITY FRAMEWORK." NUSANTARA: Jurnal Ilmu Pengetahuan Sosial 12, no. 3 (2025): 1194-1206.

¹⁶ Setyawan, D. P., & Sumari, A. D. W. S. (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum On Cybersecurity Initiatives. *Journal of Political Research*, 13(1), 1-20.

sepenuhnya sejalan dengan tingkat ancaman yang bersifat lintas negara, terorganisasi, dan melibatkan aktor dengan kemampuan serangan yang semakin canggih.

Berdasarkan hasil pembahasan, tampak bahwa Indonesia perlu memperbaiki koordinasi antarlembaga, memastikan penerapan standar keamanan digital yang konsisten di seluruh sektor, serta memperkuat kapasitas teknis dalam melakukan deteksi dini, pencegahan, dan penanganan insiden siber berskala besar. Upaya harmonisasi regulasi nasional dengan prinsip dan standar internasional juga menjadi kebutuhan mendesak, khususnya karena karakter *cyber warfare* yang tidak mengenal batas yurisdiksi dan hanya dapat dihadapi melalui pendekatan hukum yang adaptif serta kolaborasi global yang lebih intensif. Dengan demikian, penelitian ini menegaskan pentingnya penguatan fondasi hukum nasional, peningkatan kemampuan institusi yang menangani keamanan siber, serta pengembangan kerja sama internasional yang lebih strategis. Diharapkan bahwa hasil kajian ini dapat memberikan kontribusi terhadap upaya memperkuat perlindungan data dan memperkuat ketahanan infrastruktur digital Indonesia, sehingga mampu merespons berbagai bentuk ancaman *cyber warfare* yang terus berkembang dari waktu ke waktu.

DAFTAR PUSTAKA

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)

Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, 6(2), 5. Hlm 3

Mukhsin, M. (2020). Peranan teknologi informasi dan komunikasi menerapkan sistem informasi desa dalam publikasi informasi desa di era globalisasi. *Teknokom*, 3(1), 7-15.

Arianto, A. (2025). Cyber warfare dalam Konflik Modern: Analisis Serangan Stuxnet pada Fasilitas Nuklir Iran. *Dialogika: Jurnal Penelitian Komunikasi dan Sosialisasi*, 1(3), 41-52.

Febriansyah, F. I., & SH, M. (2025). Cybercrime: Kejahatan di Balik Layar Digital. *Najaha*.hlm 10

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 13(2), 222-238.

- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politika Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 10(2), 113-128.
- Rukin, S. P. (2019). Metodologi penelitian kualitatif. Yayasan Ahmar Cendekia Indonesia.
- Tahir, R., Astawa, I. G. P., Widjajanto, A., Panggabean, M. L., Rohman, M. M., Dewi, N. P. P., ... & Paminto, S. R. (2023). Metodologi penelitian bidang hukum: Suatu pendekatan teori dan praktik. PT. Sonpedia Publishing Indonesia.
- Idris, J. I., & Supandi, A. (2024). Evaluasi Kebijakan Undang-Undang Informasi dan Transaksi Elektronik di Indonesia; Potret Bibliometric Analysis. *Transparansi: Jurnal Ilmiah Ilmu Administrasi*, 7(1), 149-162.
- Pratama, A. M., Syaiful, M., & Rahman, M. F. (2024). Keamanan Data dan Informasi. Kaizen Media Publishing. Hlm 18
- Budiandru, B., & Hidayat, R. S. (2025). Tanggung Jawab Hukum Marketplace terhadap Kebocoran Data Pribadi Pengguna dalam Perspektif UU ITE dan UU Perlindungan Data Pribadi. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 4(3), 7738-7743.
- Ginanjari, Y. (2022). Strategi Indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui Badan Siber dan Sandi Negara. *Dinamika Global: Jurnal Ilmu Hubungan Internasional*, 7(02), 295-316.
- KOTA, M. K. S. D. I. LEMBAGA KETAHANAN NASIONAL REPUBLIK INDONESIA. Hlm 5
- Gunawan, R., Simangunsong, R., Susilo, T., Limbong, B., & Soeprianto, A. (2025). Penerapan Hukum Humaniter dalam Konflik Siber: Tantangan, Implikasi, dan Kebutuhan Standar Baru. *JURNAL SYNTAX IMPERATIF: Jurnal Ilmu Sosial dan Pendidikan*, 6(2), 165-173.
- Lubis, Ahmad Jufri, and Suhirwan Suhirwan. "PERANG CYBER SEBAGAI BENTUK PEPERANGAN ASIMETRIS: PERSPEKTIF FILSAFAT KEAMANAN DIGITAL DAN NIST CYBERSECURITY FRAMEWORK." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 12, no. 3 (2025): 1194-1206.
- Setyawan, D. P., & Sumari, A. D. W. S. (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum On Cybersecurity Initiatives. *Journal of Political Research*, 13(1), 1-20.