

Cyber Security Governance: Peran Organisasi Internasional dalam Pembentukan Norma Keamanan Siber Global

Cybersecurity Governance: The Role of International Organizations in Shaping Global Cybersecurity Norms

Mirza Athaya Ghaisan Hakeem¹, Muhammad Dyo Febriza², Alfarel Endito Putra³

^{1,2,3}Universitas Pembangunan Nasional “Veteran” Jakarta

E-mail: 2210611412@mahasiswa.upnvj.ac.id, 2210611429@mahasiswa.upnvj.ac.id,
2210611346@mahasiswa.upnvj.ac.id

Abstract: *The development of information and communication technology has significantly transformed global interactions but also generated complex and cross-border cyber threats, including ransomware, data theft, and critical infrastructure sabotage. The borderless nature of cyberspace makes it impossible for a single country to handle these threats independently, highlighting the need for internationally agreed norms and cybersecurity governance. Based on this context, this study aims to analyze the role of international organizations, such as the UN, ITU, NATO, OECD, and ASEAN, in establishing global cybersecurity norms and to explore the prospects for strengthening cybersecurity governance through international and regional cooperation. This research employs a normative juridical method with a literature review approach, analyzing international legal instruments, official documents of international organizations, and relevant academic literature on cybersecurity governance.*

Abstract: Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam interaksi global, namun juga menimbulkan ancaman siber yang kompleks dan lintas batas, termasuk ransomware, pencurian data, dan sabotase infrastruktur kritis. Karakter ruang siber yang tanpa batas membuat penanganan ancaman ini tidak dapat dilakukan secara individual oleh negara, sehingga diperlukan norma dan tata kelola keamanan siber yang disepakati secara internasional. Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis peran organisasi internasional, seperti PBB, ITU, NATO, OECD, dan ASEAN, dalam membentuk norma keamanan siber global serta mengeksplorasi prospek penguatan tata kelola keamanan siber melalui kerja sama internasional dan regional. Penelitian menggunakan metode yuridis normatif dengan pendekatan studi pustaka, melalui analisis terhadap instrumen hukum internasional, dokumen resmi organisasi internasional, dan literatur akademik terkait tata kelola keamanan siber.



<https://doi.org/10.5281/zenodo.17695151>

This is an open-access article under the [CC-BY-SA License](https://creativecommons.org/licenses/by-sa/4.0/).

Article History

Received: Oktober 29, 2025

Revised: November 20, 2025

Published: November 22, 2025

Keywords :

Cybersecurity, Global Governance, International Organizations, International Norms, International Cooperation

Kata Kunci :

Keamanan Siber, Tata Kelola Global, Organisasi Internasional, Norma Internasional, Kerja Sama Internasional

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah cara negara dan masyarakat berinteraksi dalam skala global. Ruang siber yang bersifat tanpa batas menciptakan peluang besar untuk inovasi dan konektivitas, namun disisi lain menimbulkan tantangan serius dalam bidang keamanan. Serangan siber yang semakin kompleks, seperti *ransomware*, pencurian data, infiltrasi sistem pemerintah, dan sabotase infrastruktur kritis, menunjukkan bahwa ancaman di ruang digital tidak dapat dipandang sebagai isu teknis semata, tetapi telah menjadi persoalan hukum dan geopolitik internasional¹.

¹ Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica: Jurnal Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 10(2), 113-128. <https://jurnal.dpr.go.id/index.php/politica/article/view/1447>

Karakter ruang siber yang lintas batas membuat suatu negara tidak dapat melindungi diri secara sepenuhnya tanpa adanya kerja sama internasional. Prinsip kedaulatan yang selama ini menjadi dasar hubungan antarnegara menghadapi tantangan baru karena tindakan di ruang siber seringkali melibatkan aktor anonim yang dapat beroperasi dari yurisdiksi mana pun. Akibatnya, negara membutuhkan landasan norma yang dapat diterima secara global untuk mengatur perilaku yang bertanggung jawab di dunia siber. Di sinilah konsep *cyber security governance* atau tata kelola keamanan siber menjadi kunci dalam menjaga stabilitas dan keamanan global.²

Dalam proses pembentukan tata kelola tersebut, organisasi internasional memegang peran yang sangat penting. Perserikatan Bangsa-Bangsa (PBB), melalui forum *UN global cyber norm* seperti *United Nations Group of Governmental Experts* (UNGGE) dan *Open Ended Working Group* (OEWG), berupaya menetapkan prinsip-prinsip perilaku negara yang dianggap sah dan bertanggung jawab di ruang siber. Di sisi lain, *International Telecommunication Union* (ITU) mengembangkan standar teknis dan kebijakan global, sementara *North Atlantic Treaty Organization* (NATO) memperkuat aspek pertahanan siber melalui doktrin kolektif. *Organisation for Economic Co-operation and Development* (OECD) memberikan pedoman tata kelola informasi yang diadopsi banyak negara, dan *Association of Southeast Asia Nation* (ASEAN) berupaya membangun kerangka kerja regional untuk meningkatkan kesiapsiagaan negara-negara Asia Tenggara. Kehadiran organisasi ini memungkinkan terciptanya harmonisasi awal terkait norma keamanan siber³.

Namun demikian, upaya pembentukan norma keamanan siber global tidak berjalan mudah. Perbedaan kepentingan negara-negara besar, misalnya antara negara yang mengusung prinsip *open and free internet* dengan negara yang lebih menekankan konsep *cyber sovereignty*, menyebabkan penyusunan norma global seringkali terhambat. Selain itu, kesenjangan kapasitas teknologi antara negara maju dan negara berkembang ikut mempengaruhi kemampuan dalam menerapkan standar keamanan siber internasional. Isu atribusi serangan siber yang sulit dibuktikan juga membuat penegakan hukum di tingkat internasional menjadi tidak efektif.

Kondisi ini menimbulkan pertanyaan penting mengenai efektivitas organisasi internasional dalam membentuk tata kelola keamanan siber yang inklusif, stabil, dan dapat diterima oleh seluruh negara. Diperlukan koordinasi yang lebih kuat serta pendekatan kolaboratif untuk menyelaraskan kepentingan politik, standar teknis, dan kapasitas hukum antarnegara. Dengan demikian, pembentukan norma global tidak hanya bersifat deklaratif tetapi juga implementatif, terutama dalam menghadapi serangan siber yang semakin mengancam stabilitas nasional dan internasional.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada dua masalah utama: bagaimana peran organisasi internasional dalam merumuskan norma keamanan siber global, serta bagaimana prospek dan strategi penguatan tata kelola keamanan siber melalui kerja sama internasional dan regional. Dengan menggunakan metode penelitian yuridis normatif, artikel ini akan menganalisis instrumen hukum internasional, kebijakan organisasi internasional, serta literatur akademik untuk memahami perkembangan dan arah tata kelola keamanan siber global ke depan.

RUMUSAN MASALAH

Berdasarkan latar belakang yang sudah dijelaskan diatas maka dapat dirumuskan masalah sebagai berikut:

² Maesaroh, R. S. (2024). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(2). <https://ejournal.uin-suka.ac.id/syariah/Staatsrecht/article/view/3980>

³ Suadhana Rai, I. N. A., Heryadi, D., & Kamaluddin, A. N. (2022). Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber. *Politica*, 13(1), 43–66. <https://jurnal.dpr.go.id/index.php/politica/article/view/2641>

1. Bagaimana peran organisasi internasional, seperti PBB, ITU, NATO, OECD, dan ASEAN, dalam merumuskan serta membentuk norma-norma keamanan siber global?
2. Bagaimana prospek dan strategi penguatan tata kelola keamanan siber global melalui kerja sama internasional dan regional di masa mendatang?

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis normatif, yaitu penelitian yang berfokus pada kajian terhadap norma, prinsip, dan aturan hukum yang berkaitan dengan tata kelola keamanan siber global (*cyber security governance*). Pendekatan yuridis normatif ini digunakan untuk menganalisis bagaimana organisasi internasional membentuk norma dan standar hukum yang berkaitan dengan keamanan siber.

HASIL PEMBAHASAN

1. Peran organisasi internasional, seperti PBB, ITU, NATO, OECD, dan ASEAN, dalam merumuskan serta membentuk norma-norma keamanan siber global.

Perkembangan teknologi digital telah membawa ancaman keamanan yang semakin kompleks dan lintas batas. Serangan siber tidak lagi hanya menasar infrastruktur teknis, tetapi sudah berkaitan dengan stabilitas politik, ekonomi, dan pertahanan negara. Kondisi ini menuntut adanya norma dan kesepakatan internasional agar negara tidak menangani ancaman secara terpisah-pisah. Berbagai penelitian di Indonesia menunjukkan bahwa pembentukan tata kelola keamanan siber global tidak dapat dilakukan oleh satu negara saja, sehingga peran organisasi internasional menjadi sangat penting dalam merumuskan standar, prinsip, dan arah kebijakan keamanan siber dunia.

PBB dianggap sebagai ruang utama pembentukan norma global karena lembaga ini menjadi forum resmi negara-negara untuk menyepakati prinsip hukum yang berlaku di ruang digital. Melalui mekanisme seperti *Group of Governmental Experts* (GGE) dan *Open-Ended Working Group* (OEWG), PBB berhasil mendorong kesepakatan mengenai penerapan hukum internasional, tanggung jawab negara dalam mencegah serangan dari wilayahnya, serta pentingnya perlindungan terhadap infrastruktur sipil. Penelitian akademik dalam negeri menilai bahwa norma-norma ini menjadi “bahasa bersama” yang digunakan negara dalam diplomasi siber, termasuk oleh Indonesia, sehingga PBB berperan sebagai pemberi legitimasi politik terhadap prinsip dasar keamanan siber.

Di samping itu, perumusan norma global perlu diterjemahkan ke dalam standar teknis agar dapat diimplementasikan. Di titik inilah peran *International Telecommunication Union* (ITU) menjadi signifikan. Lembaga ini memberikan dukungan teknis melalui program penilaian, asistensi, dan penyusunan standar, salah satunya melalui *Global Cybersecurity Index* (GCI). Indonesia, sebagaimana disorot beberapa jurnal nasional, memanfaatkan GCI untuk menilai kematangan keamanan sibernya sekaligus sebagai tolok ukur pembangunan kapasitas nasional. Dengan demikian, ITU menjalankan fungsi pelengkap PBB: dari kesepakatan hukum menuju kesiapan teknis⁴.

Berbeda dari kedua lembaga tersebut, NATO menempatkan keamanan siber dalam konteks pertahanan kolektif. Sebagai aliansi militer, NATO menjadi organisasi internasional pertama yang secara tegas menyatakan bahwa serangan siber dapat dipandang sebagai tindakan

⁴ Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Populis: Jurnal Sosial Dan Humaniora*, 8(1), 57-73.

agresi yang memicu respons bersama. Melalui kajian, simulasi, dan pengembangan standar di NATO *Cooperative Cyber Defence Centre of Excellence*, organisasi ini membantu negara-negara membangun pemahaman strategis tentang eskalasi serangan, manajemen konflik siber, serta prosedur pertahanan. Penelitian Indonesia menyebut bahwa doktrin NATO kemudian menjadi rujukan banyak negara saat membangun postur pertahanan siber nasional, meskipun Indonesia bukan anggota aliansi tersebut⁵.

Namun, pengembangan norma siber tidak hanya berkaitan dengan pertahanan dan hukum internasional. Organisasi seperti OECD memberikan perspektif berbeda, yakni menjadikan keamanan siber sebagai prasyarat stabilitas ekonomi digital. Melalui kebijakan yang menekankan manajemen risiko, perlindungan konsumen, dan partisipasi sektor swasta, OECD mengingatkan bahwa keamanan digital bukan hanya domain pemerintah, tetapi ekosistem yang harus dijaga bersama. Kajian hukum Indonesia menunjukkan bahwa pendekatan OECD membantu negara tidak terjebak dalam keamanan yang bersifat militeristik, melainkan menempatkan ruang digital sebagai ruang konstruksi ekonomi yang harus dikelola secara sehat.

Sementara itu, ASEAN menunjukkan bagaimana norma global harus disesuaikan ketika diterapkan pada tingkat regional. Negara-negara Asia Tenggara memiliki kapasitas pertahanan siber yang berbeda-beda, sehingga ASEAN lebih menekankan kerja sama yang bersifat praktis, seperti pertukaran informasi insiden, pelatihan keamanan, harmonisasi kebijakan, dan confidence-building measures. Penelitian mengenai diplomasi siber Indonesia memperlihatkan bahwa forum seperti *ASEAN Ministerial Conference on Cybersecurity* dan *ASEAN Regional Forum* menjadi sarana memperkuat kepercayaan antarnegara, karena tantangan siber di kawasan tidak dapat diselesaikan hanya dengan regulasi nasional⁶.

Peran ASEAN juga dapat dilihat dari langkahnya memfokuskan penguatan sumber daya manusia serta peningkatan kesiapan teknis negara anggota. Hal ini dinilai sejalan dengan kondisi negara Asia Tenggara yang sebagian masih menghadapi keterbatasan teknologi dan perangkat hukum. Karena itu, kontribusi ASEAN tidak terletak pada penyusunan doktrin atau aturan hukum yang bersifat mengikat, tetapi pada pendekatan penguatan kapasitas yang memungkinkan negara berkembang mampu mencapai standar yang ditetapkan dalam forum global yang lebih luas.

Jika dibandingkan satu sama lain, tampak bahwa pembentukan norma keamanan siber global merupakan proses bertahap yang memerlukan pembagian fungsi di antara berbagai organisasi dunia⁷. PBB memberikan legitimasi hukum dan kerangka prinsip yang disepakati negara-negara. ITU memastikan bahwa negara memiliki instrumen teknis untuk menerjemahkan prinsip tersebut ke tingkat implementasi. NATO memperkuat standar dalam konteks pertahanan dan keamanan kolektif. OECD mengaitkannya dengan tata kelola ekonomi digital, sementara ASEAN menerjemahkannya ke dalam model kerja sama regional yang lebih realistis bagi negara berkembang.

Meskipun demikian, berbagai penelitian dari Indonesia juga menegaskan bahwa proses ini tidak bebas hambatan. Perbedaan kepentingan geopolitik, sensitivitas nasional terhadap isu kedaulatan data, serta kesenjangan kemampuan teknologi antarnegara menyebabkan tidak

⁵ Putri, E., Pratama, G. A., & Fithri, B. S. (2023). Keamanan Nasional dalam Menghadapi Perubahan *Cyber Warfare*. *JURNAL MERCATORIA*, 16(2), 201-2

⁶ Anny Susilowati. (2025). Penegakan Hukum Internasional terhadap Serangan Siber terhadap Infrastruktur Kritis di Indonesia. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, 2(5), 122–141. <https://doi.org/10.62383/aliansi.v2i5.1204>

⁷ Kristianti, N., & Kurniasi, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma: Jurnal Ilmu Hukum*, 7(1), 297-310.

semua norma dapat diterapkan secara seragam. Di samping itu, tidak adanya lembaga penegak global juga membuat norma keamanan siber masih bergantung pada komitmen politik negara masing-masing. Karena itu, pembentukan norma siber global harus dipandang sebagai proses evolutif, yang terus bergantung pada dinamika politik, ekonomi, serta perkembangan teknologi itu sendiri.

Dari uraian tersebut dapat disimpulkan bahwa organisasi internasional memiliki peran yang berbeda tetapi saling melengkapi dalam membangun tatanan keamanan siber global. Melalui interaksi antar organisasi inilah masyarakat internasional berusaha membentuk mekanisme tata kelola yang tidak hanya sah secara hukum, namun juga dapat diimplementasikan secara teknis, diterima secara politik, dan relevan bagi negara di berbagai tingkat kemampuan⁸.

2. Prospek dan strategi penguatan tata kelola keamanan siber global melalui kerja sama internasional dan regional di masa mendatang

Dalam menghadapi ancaman siber yang semakin kompleks dan transnasional, prospek penguatan tata kelola keamanan siber global sangat bergantung pada peningkatan kerja sama lintas negara dan lintas institusi. Strategi ke depan harus mengintegrasikan diplomasi siber yang bersifat multilateral, bilateral, dan multi stakeholder, karena tidak ada satu negara pun yang mampu mengatasi sendiri risiko-risiko siber global⁹.

Salah satu strategi utama adalah memperkuat kapasitas teknis negara-negara berkembang melalui kerangka kerja yang diprakarsai oleh organisasi seperti ITU. Kerja sama teknis dalam bentuk pelatihan, asistensi standar, dan pertukaran pengalaman akan sangat menentukan sejauh mana negara-negara dengan kapasitas terbatas bisa mengadopsi norma internasional dan meningkatkan ketahanan siber nasional¹⁰. Dalam konteks Indonesia, penguatan kelembagaan BSSN (Badan Siber dan Sandi Negara) telah menjadi kunci dalam tata kelola nasional dan diplomasi siber, sehingga lembaga nasional dapat berfungsi sebagai mitra aktif dalam kerjasama global.

Pada tingkat regional, ASEAN memiliki prospek strategis besar untuk memperkuat tata kelola keamanan siber melalui mekanisme kerja sama yang lebih intensif. Melalui *ASEAN Regional Forum* (ARF) dan strategi keamanan siber kawasan, negara anggota dapat membangun mekanisme pertukaran intelijen insiden siber, latihan siber bersama, serta penerapan *confidence-building measures*¹¹. Penelitian yang dilakukan oleh beberapa ahli menyebut bahwa upaya diplomasi pertahanan siber Indonesia di forum ASEAN telah mengarah pada format kerja sama yang konkret, seperti penunjukan point of contacts antar negara dan penyelenggaraan workshop keamanan siber.

Prospek lain adalah diplomasi bilateral yang lebih strategis. Misalnya, kerjasama siber antara Indonesia dan Inggris pada periode 2018–2028 mencakup aspek peningkatan kapasitas sumber daya manusia melalui pelatihan “*cyber law*”, pembentukan CSIRT (*Computer Security Incident Response Team*), dan awareness siber publik¹². Pendekatan bilateral semacam ini

⁸ Rachmawiana, M. (2025). Kebijakan Indonesia Dalam Kerjasama Dengan Amerika Serikat di Bidang Siber Tahun 2023-2024. *Global Insights Journal : Jurnal Mahasiswa Hubungan Internasional*, 2(1). <https://ejournal.fisip.unjani.ac.id/index.php/GIJ/article/view/4217>

⁹ Soeroto, R. A. (2025). Strategi Diplomati Internasional Menghadapi Tantangan Keamanan Siber. *Jurnal Cakrawala Ilmiah*, 4(7), 1095-1104.

¹⁰ Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica: Jurnal Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 10(2), 113–128. <https://jurnal.dpr.go.id/index.php/politica/article/view/1447>.

¹¹ Damareka. 2023. “Peran Organisasi Internasional Dalam Memperkuat Pertahanan Siber Global Pada Negara Berkembang.” *Media Hukum Indonesia*.

¹² Nurdianto, R. A., Subagyo, A., & Sari, S. (2024). Kerjasama Keamanan Siber Indonesia-Inggris Pada Periode 2018-2028.

memungkinkan negara-negara untuk secara langsung menyesuaikan kerja sama dengan kebutuhan nasional sambil berkontribusi pada tata kelola global melalui pertukaran praktik terbaik.

Tata kelola global juga akan semakin membutuhkan kerangka hukum internasional yang lebih kuat dan formal. Strategi ini mencakup negosiasi perjanjian multinasional mengikat yang menarget isu-isu mutakhir seperti serangan ransomware lintas negara, rantai pasokan perangkat lunak, dan ketergantungan pada platform digital besar. Penegakan hukum internasional terhadap serangan pada infrastruktur kritis menjadi sangat penting; dalam studi oleh Susilowati dan Rahmawati, mereka menemukan hambatan perlindungan hukum karena kedaulatan negara, regulasi yang belum jelas, dan kurangnya kesepahaman antarnegara¹³.

Selain itu, penguatan tata kelola siber global harus mempertimbangkan relevansi nilai-nilai lokal dan nasional. Harmonisasi regulasi internasional dengan kepentingan nasional Indonesia, misalnya berdasarkan nilai Pancasila, menjadi strategi penting agar norma global dapat diterima secara domestik.¹⁴ Para ahli dan pengamat menyoroti bagaimana peraturan internasional dan kepentingan kedaulatan digital Indonesia bisa diseimbangkan melalui pendekatan regulatif yang menghormati nilai-nilai lokal.

Dalam aspek kelembagaan nasional, penguatan BSSN sebagai lembaga cyber nasional sangat strategis untuk menjembatani kerja sama global dan regional. Harus diketahui bahwa BSSN memiliki peran vital dalam menjaga kedaulatan siber dan merespons ancaman internasional, tetapi diperlukan reformasi kelembagaan, penguatan anggaran, dan peningkatan mandat melalui undang-undang agar dapat lebih efektif sebagai aktor tata kelola global¹⁵.

Di sisi pertahanan nasional, strategi penguatan kerja sama internasional dan regional juga harus menyasar peningkatan koordinasi antar lembaga domestik. Menurut penelitian di Jurnal Dinamika Global, upaya Indonesia harus mencakup koordinasi lintas instansi pemerintah, kerja sama dengan sektor swasta, serta pelibatan masyarakat sipil dalam keamanan siber. Kolaborasi semacam itu tidak hanya memperkuat sistem pertahanan internal, tetapi juga memperkuat posisi Indonesia dalam tata kelola keamanan siber global.

Terakhir, prospek tata kelola keamanan siber global sangat tergantung pada keberlanjutan kerjasama *multi stakeholder*, yang melibatkan pemerintah, sektor swasta, akademisi, dan masyarakat sipil. Organisasi internasional dan regional harus membuka ruang bagi semua pemangku kepentingan untuk berpartisipasi dalam pembentukan norma dan mekanisme. Dengan demikian, strategi masa depan harus menjaga keseimbangan antara agenda geopolitik, kepentingan nasional, dan kepentingan kolektif dalam membangun tatanan siber yang stabil, inklusif, dan adaptif.

SIMPULAN

Pembentukan norma keamanan siber global merupakan proses kolektif yang tidak dapat dijalankan oleh satu negara saja, melainkan memerlukan peran berbagai organisasi internasional dengan fungsi yang saling melengkapi. PBB berperan sebagai forum legitimasi hukum dan politik melalui perumusan prinsip-prinsip dasar dalam ruang siber, sementara ITU menerjemahkannya ke dalam standar dan kesiapan teknis negara. NATO memperkuat dimensi pertahanan dan respons kolektif atas

¹³ Anny Susilowati. (2025). Penegakan Hukum Internasional terhadap Serangan Siber terhadap Infrastruktur Kritis di Indonesia. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, 2(5), 122–141. <https://doi.org/10.62383/aliansi.v2i5.1204>

¹⁴ Abdurrohman, A. H., Uzmawi, C. N., Khoiruddin, R., Nasoha, A. M. M., & Atqiya, A. N. (2025). Cybersecurity dan Pancasila: Harmonisasi Regulasi Hukum Internasional dengan Kepentingan Nasional. *JDHI: Jurnal Dinamika Hukum Indonesia*, 1(1), 23–29.

¹⁵ Cyberthreat.id. 2023. "BSSN Susun Roadmap Kerja Sama Internasional Bidang Keamanan Siber." <https://cyberthreat.id/read/15962/BSSN-Susun-Roadmap-Kerja-Sama-Internasional-Bidang-Keamanan-Siber>

serangan siber, OECD menghadirkan pendekatan berbasis tata kelola ekonomi digital, dan ASEAN menyesuakannya dalam bentuk kerja sama regional yang lebih realistis bagi negara berkembang, termasuk Indonesia. Meskipun menghadapi tantangan berupa perbedaan kepentingan geopolitik, kesenjangan kapasitas teknologi, dan belum adanya lembaga penegak global yang kuat, norma keamanan siber terus berkembang secara dinamis. Dengan demikian, tata kelola keamanan siber global saat ini terbentuk melalui interaksi antara kepentingan hukum, teknis, pertahanan, ekonomi, dan regional yang saling berkaitan.

SARAN

Pemerintah Indonesia perlu memperkuat posisi dan perannya dalam tata kelola keamanan siber global dengan meningkatkan partisipasi aktif di forum multilateral seperti PBB, ITU, dan ASEAN, sekaligus memperluas kerja sama bilateral yang strategis dalam bidang keamanan siber. Penguatan kelembagaan BSSN harus menjadi prioritas melalui peningkatan wewenang hukum, sumber daya manusia, dan dukungan anggaran agar mampu berperan optimal di tingkat nasional maupun internasional. Selain itu, pemerintah perlu mendorong sinkronisasi regulasi nasional dengan norma internasional tanpa mengabaikan nilai-nilai kedaulatan dan kepentingan nasional, serta memperkuat koordinasi lintas kementerian/lembaga agar strategi keamanan siber nasional berjalan lebih terintegrasi dan adaptif terhadap perkembangan ancaman global.

REFERENSI

- Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). *Populis: Jurnal Sosial Dan Humaniora*, 8(1), 57-73.
- Putri, E., Pratama, G. A., & Fithri, B. S. (2023). Keamanan Nasional dalam Menghadapi Perubahan Cyber Warfare. *JURNAL MERCATORIA*, 16(2), 201-208.
- Anny Susilowati. (2025). Penegakan Hukum Internasional terhadap Serangan Siber terhadap Infrastruktur Kritis di Indonesia. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, 2(5), 122–141. <https://doi.org/10.62383/aliansi.v2i5.1204>
- Kristianti, N., & Kurniasi, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma: Jurnal Ilmu Hukum*, 7(1), 297-310.
- Rachmawiana, M. (2025). Kebijakan Indonesia Dalam Kerjasama Dengan Amerika Serikat di Bidang Siber Tahun 2023-2024. *Global Insights Journal : Jurnal Mahasiswa Hubungan Internasional*, 2(1). Retrieved from <https://ejournal.fisip.unjani.ac.id/index.php/GIJ/article/view/4217>
- ANTARA News. 2020. *Indonesia di PBB serukan pentingnya stabilitas siber*. <https://www.antaranews.com/berita/1511830/indonesia-di-pbb-serukan-pentingnya-stabilitas-siber>.
- Perwakilan PBB Indonesia. 2025. *Pengarahannya Pasca-Konvensi PBB Melawan Kejahatan Dunia Maya*. <https://indonesia.un.org/id/290254-pengarahannya-pasca-konvensi-pbb-melawan-kejahatan-dunia-maya-sambutan-kepala-perwakilan-pbb>.
- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica: Jurnal Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 10(2), 113–128. <https://jurnal.dpr.go.id/index.php/politica/article/view/1447>.
- Maesaroh, R. S. (2024). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum*

- Kenegaraan dan Politik Islam, 4(2). <https://ejournal.uin-suka.ac.id/syariah/Staatsrecht/article/view/3980>
- Damareka. 2023. "Peran Organisasi Internasional Dalam Memperkuat Pertahanan Siber Global Pada Negara Berkembang." *Media Hukum Indonesia*. <https://ojs.daarulhuda.or.id/index.php/MHI/article/view/1759>
- Cyberthreat.id. 2023. "BSSN Susun Roadmap Kerja Sama Internasional Bidang Keamanan Siber." <https://cyberthreat.id/read/15962/BSSN-Susun-Roadmap-Kerja-Sama-Internasional-Bidang-Keamanan-Siber>.
- Galang Ramadhan, *Analisis Strategi Keamanan Nasional Indonesia dalam Menghadapi Ancaman Siber*, *Jurnal Konstitusi*. <https://ejournal.appihi.or.id/index.php/Konstitusi/article/view/722> EJournal APPHI
- Saepudin Hidayat & Aris Setyo Radyawanto, *Kemandirian Siber Indonesia: Tantangan dan Peluang Menuju Kedaulatan Digital*, *International Journal of Social and Management Studies*. <https://www.ijosmas.org/index.php/ijosmas/article/view/537>.
- Soeroto, R. A. (2025). Strategi Diplomati Internasional Menghadapi Tantangan Keamanan Siber. *Jurnal Cakrawala Ilmiah*, 4(7), 1095-1104.
- Nurdiyanto, R. A., Subagyo, A., & Sari, S. (2024). Kerjasama Keamanan Siber Indonesia-Inggris Pada Periode 2018-2028. *Diplomacy and Global Security Journal : Jurnal Mahasiswa Magister Hubungan Internasional*, 1(1). <https://doi.org/https://doi.org/10.36859/dgsj.v1i1.2889>
- Abdurrohman, A. H., Uzmawi, C. N., Khoiruddin, R., Nasoha, A. M. M., & Atqiya, A. N. (2025). Cybersecurity dan Pancasila: Harmonisasi Regulasi Hukum Internasional dengan Kepentingan Nasional. *JDHI: Jurnal Dinamika Hukum Indonesia*, 1(1), 23-29.