Legal Note
Vol. 1 No. 2, October 2025, pages: 31-36
e-ISSN 3110-2344 | DOI: https://doi.org/10.71094/legalnote.v1i1.100

Kedaulatan Siber: Tantangan dan Implikasi terhadap Hukum Internasional Modern

Indra Duari [*1], Muhammad Saiful [1], Heri Pratama [1]
Program Hukum internasional Fakultas Hukum Universitas Atma Jaya Yogyakarta
**Corresponding Author: duari22@gmail.com*

Article History

Manuscript submitted:
15 October, 2025
Manuscript revised:
20 October, 2025
Accepted for publication:
30 October, 2025

Keywords

Cyber Sovereignty;
International Law;
Digital Security;
Tallinn Manual;
State Sovereignty;

Abstract

The rapid development of information and communication technology has created a new dimension in the global order—cyberspace, which has become a strategic arena in international relations. This phenomenon raises fundamental questions regarding the concept of state sovereignty in cyberspace and how international law governs it. This study aims to analyze the principles of sovereignty within the cyber context and their implications for modern international legal frameworks. The research employs a normative approach by examining various international legal instruments such as the UN Charter, the Tallinn Manual 2.0, and conventions related to cybersecurity. The findings reveal that cyber sovereignty is not explicitly regulated in existing international legal instruments; however, the fundamental principles of state sovereignty remain applicable in this domain. Actions such as cyberattacks between states may be categorized as violations of sovereignty or even acts of aggression if they threaten a nation's security. Moreover, there is an ongoing tension between national security interests and the principle of freedom of expression as recognized in international law. This study concludes that there is an urgent need for the establishment of more specific international legal norms to govern cyber activities, in order to prevent inter-state conflicts and ensure that the fundamental principles of international law are upheld in the digital era. The creation of a global legal framework for fair, inclusive, and transparent cyber governance is essential to promote stability and justice in modern international relations.

How to Cite: Duari, I., Saiful, M., & Pratama, H. (2025). Kedaulatan Siber: Tantangan dan Implikasi terhadap Hukum Internasional Modern. *Legal Note, 1*(2), 31–36. https://doi.org/10.71094/legalnote.v1i1.100

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang cepat telah memperluas konsep ruang internasional ke dalam domain siber. Ruang siber bukan hanya sekadar alat komunikasi atau pertukaran data, melainkan sebuah arena di mana interaksi antarnegara, aktor-aktor non-negara, dan bahkan individu berlangsung dengan konsekuensi yang sangat nyata terhadap keamanan, hak asasi manusia, dan kedaulatan negara. Sejauh mana negara-negara dapat mempertahankan kontrol atas wilayah digital dan infrastrukturnya menjadi masalah hukum dan politik yang semakin mendesak. Dalam konteks ini muncul istilah cyber sovereignty, yaitu hak suatu negara untuk mengatur, melindungi, dan mengawasi aktivitas siber di dalam wilayahnya sendiri dan dalam hubungannya dengan negara-negara lain.

Istilah sovereignty dalam hukum internasional tradisional merujuk pada kekuasaan tertinggi suatu negara atas wilayahnya—baik internal (pengaturan domestik) maupun eksternal (pengakuan dan interaksi dengan negara lain). Namun, ruang siber menantang beberapa asumsi dasar dari konsep ini: misalnya, tidak selamanya ada batas geografis yang jelas; data dan sinyal dapat melintasi batas negara secara instan; dan seringkali infrastruktur siber dimiliki oleh pihak swasta atau multinasional, sehingga pertanyaan hukum dan regulatif menjadi kompleks. Schmitt dan Vihul (2017) menulis bahwa meskipun prinsip kedaulatan bersifat fundamental, aplikasinya dalam domain siber belum sepenuhnya jelas, terutama mengenai bagaimana kedaulatan terwujud dalam praktik di bawah ambang penggunaan kekuatan (use of force) atau intervensi. centaur.reading.ac.uk

Selain itu, terdapat juga perdebatan apakah operasi siber yang tidak menyebabkan kerusakan fisik langsung tetap dapat dianggap sebagai pelanggaran kedaulatan suatu negara. Kevin Jon Heller (2021) mendiskusikan tiga pendekatan utama dalam posisi internasional terhadap operasi siber tingkat rendah (low-intensity cyber operations): bahwa operasi tersebut tidak pernah salah secara hukum karena kedaulatan dianggap bukan aturan primer yang dapat dilanggar; bahwa operasi tersebut selalu salah; dan pendekatan relatif, yakni hanya salah jika ada efek fisik atau inoperabilitas infrastruktur negara target. digital-commons.usnwc.edu Perdebatan ini menggambarkan bagaimana norma hukum internasional mencoba untuk beradaptasi dengan fenomena baru yang belum sepenuhnya terakomodasi dalam instrumen hukum yang ada.

Instrumen hukum internasional seperti Piagam Perserikatan Bangsa-Bangsa (PBB), berbagai konvensi HAM, serta dokumen-normatif seperti Tallinn Manual 2.0 telah menjadi referensi penting untuk melihat bagaimana norma-norma hukum diterapkan dalam konteks siber. Tallinn Manual misalnya menyajikan sejumlah aturan "[black-letter rules]" yang mencoba menerjemahkan norma hukum internasional ke dalam konteks perang siber dan operasi siber antarnegara. Cambridge University Press & Assessment+2centaur.reading.ac.uk+2 Namun demikian, sifatnya yang tidak mengikat (non-binding) dan kekurangan praktik negara (state practice) yang konsisten masih menjadi hambatan bagi pembentukan norma hukum siber yang definitif. Chatham House+1

Tantangan praktis muncul juga dari fakta bahwa banyak serangan atau intrusi siber yang dilakukan oleh aktor non-negara atau aktor yang beroperasi di luar kontrol negara tertentu, sehingga sulit menentukan tanggung jawab hukum negara atau siapa yang harus diwajibkan untuk mempertahankan norma internasional dalam kasus-kasus seperti itu. Prinsip non-intervensi dan kedaulatan teritorial menjadi pusat kontroversi ketika tindakan siber melibatkan gangguan tanpa izin ke sistem komputer atau infrastruktur digital negara lain. Chatham House+1

Lebih jauh, ketegangan muncul antara kepentingan keamanan nasional dan hak asasi manusia di ruang siber. Misalnya, negara mungkin berusaha memperketat kontrol atas arus data, mensensor konten, atau melakukan pengawasan digital dengan dalih melindungi keamanan nasional, namun tindakan ini dapat berbenturan dengan prinsip kebebasan berekspresi, privasi, dan hak atas informasi sebagaimana diakui dalam hukum internasional hak asasi manusia. Konflik ini memperlihatkan bahwa hukum internasional modern perlu menemukan keseimbangan antara regulasi siber yang ketat dan penghormatan terhadap hak fundamental.

Dalam kerangka hukum internasional kontemporer, terdapat kebutuhan yang semakin jelas untuk pembentukan norma hukum yang lebih spesifik dan adaptif terhadap karakteristik domain siber: cross-border, cepat berubah, dengan aktor non-negara yang signifikan, dan banyaknya perisai hukum domestik yang berbeda antarnegara. Pendekatan multilateral dan inklusif menjadi sangat penting, agar norma yang dibentuk mendapat legitimasi global dan dapat diimplementasikan secara konsisten. Kerangka hukum global tentang cyber governance yang adil, transparan dan inklusif (termasuk mekanisme akuntabilitas

dan penyelesaian sengketa) menjadi tumpuan agar hubungan internasional digital berjalan dengan stabil dan adil.

Akhirnya, penelitian ini bertujuan untuk menggali: (1) bagaimana prinsip-prinsip kedaulatan negara diterjemahkan dalam konteks siber oleh negara dan komunitas internasional; (2) sejauh mana instrumen hukum internasional yang ada (termasuk norma tidak tertulis atau praktik negara) mampu mengatur aktivitas siber, terutama operasi siber yang berada di bawah ambang kekerasan dan intervensi; dan (3) apa implikasi praktis dan teoretis jika norma hukum baru atau adaptasi norma lama diperlukan untuk memastikan keamanan, keadilan, dan penghormatan terhadap kedaulatan serta hak asasi manusia di era digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan normatif yuridis, yaitu metode yang menitikberatkan pada kajian terhadap norma-norma hukum positif, prinsip-prinsip hukum internasional, serta instrumen hukum yang mengatur kedaulatan negara di ruang siber. Pendekatan ini dipilih karena isu kedaulatan siber merupakan ranah hukum yang masih dalam proses pembentukan norma dan interpretasi hukum internasional. Peneliti menganalisis dokumen hukum primer seperti Piagam Perserikatan Bangsa-Bangsa (PBB), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, serta konvensi internasional terkait keamanan informasi. Pendekatan normatif digunakan untuk menilai sejauh mana norma-norma yang ada dapat diterapkan pada aktivitas siber antarnegara (Schmitt, 2017).

Jenis penelitian ini adalah penelitian kualitatif deskriptif, di mana data dikumpulkan dan dianalisis secara mendalam untuk memberikan pemahaman komprehensif mengenai hubungan antara kedaulatan negara dan aktivitas siber. Data yang digunakan terdiri atas data sekunder, yang meliputi bahan hukum primer, sekunder, dan tersier. Bahan hukum primer mencakup peraturan dan konvensi internasional; bahan hukum sekunder berupa buku, jurnal, dan artikel akademik yang membahas hukum siber; sedangkan bahan hukum tersier meliputi kamus hukum dan ensiklopedia internasional (Bryman, 2016).

Teknik pengumpulan data dilakukan melalui studi kepustakaan (library research). Peneliti menelaah literatur ilmiah yang relevan dari berbagai sumber, termasuk publikasi lembaga internasional seperti International Telecommunication Union (ITU) dan United Nations Office on Drugs and Crime (UNODC) yang membahas tata kelola siber global. Selain itu, artikel ilmiah yang diterbitkan dalam jurnal bereputasi seperti Journal of Cyber Policy dan International Law Studies juga dijadikan rujukan untuk memperkuat dasar teori dan argumentasi (Tikk et al., 2018).

Analisis data dilakukan dengan menggunakan metode analisis kualitatif terhadap bahan hukum (content analysis). Proses ini melibatkan pengumpulan, klasifikasi, dan interpretasi terhadap data hukum serta doktrin yang berkaitan dengan isu kedaulatan di ruang siber. Analisis ini bertujuan untuk mengidentifikasi kesenjangan antara norma hukum internasional yang ada dan realitas praktik yang berkembang di dunia maya. Peneliti juga mengkaji perbandingan antara pendekatan hukum internasional tradisional dengan paradigma baru dalam tata kelola siber global (Tsagourias & Buchan, 2015).

Untuk menjaga validitas hasil penelitian, dilakukan triangulasi sumber dengan cara membandingkan berbagai dokumen dan pendapat ahli hukum internasional. Pendekatan ini digunakan untuk memastikan bahwa interpretasi yang dihasilkan tidak bersifat subjektif semata, melainkan berdasarkan konsensus akademik dan norma hukum yang diakui secara internasional. Dengan demikian, penelitian ini tidak hanya menggambarkan kondisi aktual, tetapi juga memberikan kontribusi terhadap pengembangan teori hukum internasional di bidang kedaulatan siber (Kleffner, 2013).

Akhirnya, penelitian ini diharapkan mampu menghasilkan kerangka analisis hukum yang komprehensif mengenai tantangan kedaulatan negara dalam ruang siber. Melalui metode normatif yuridis dan analisis kualitatif, penelitian ini berupaya memperkuat pemahaman tentang hubungan antara hukum internasional dan keamanan digital global. Hasil penelitian ini diharapkan dapat menjadi rujukan bagi

pembuat kebijakan, akademisi, dan lembaga internasional dalam merumuskan aturan hukum yang adaptif dan responsif terhadap perkembangan teknologi siber di masa depan (Choucri, 2012).

HASIL DAN PEMBAHASAN

Perkembangan pesat teknologi informasi dan komunikasi telah mengubah secara fundamental cara negara berinteraksi dan melindungi kedaulatannya. Dalam konteks hukum internasional, konsep kedaulatan yang sebelumnya hanya diterapkan pada wilayah fisik kini diperluas ke ruang siber yang bersifat tanpa batas. Ruang siber menjadi area strategis baru bagi kepentingan politik, ekonomi, dan pertahanan nasional, yang menuntut adanya regulasi dan norma hukum internasional yang adaptif terhadap tantangan digital (Krasner, 2020). Dalam beberapa dekade terakhir, isu mengenai kedaulatan siber menjadi sorotan utama karena meningkatnya insiden serangan siber antarnegara, seperti yang terjadi antara Rusia dan Ukraina, maupun antara Amerika Serikat dan Tiongkok.

Hasil analisis menunjukkan bahwa tidak ada instrumen hukum internasional yang secara eksplisit mengatur kedaulatan di ruang siber. Namun, prinsip dasar kedaulatan sebagaimana tertuang dalam Piagam Perserikatan Bangsa-Bangsa (PBB) tetap relevan dan dapat diterapkan dalam konteks siber. Menurut prinsip tersebut, setiap negara memiliki hak penuh atas yurisdiksi dan pengendalian terhadap aktivitas dalam batas wilayahnya, termasuk jaringan dan infrastruktur digitalnya (Schmitt, 2017). Dalam praktiknya, banyak negara mulai mengembangkan kebijakan nasional tentang keamanan siber yang berlandaskan pada prinsip kedaulatan digital, meskipun hal ini sering menimbulkan perdebatan tentang batas antara pengawasan dan pelanggaran hak asasi manusia.

Selain itu, penelitian menunjukkan bahwa Tallinn Manual 2.0 menjadi salah satu rujukan penting dalam memahami penerapan hukum internasional terhadap operasi siber. Dokumen ini menyatakan bahwa serangan siber yang mengakibatkan kerusakan fisik atau gangguan signifikan terhadap infrastruktur vital dapat dianggap sebagai pelanggaran terhadap kedaulatan suatu negara (Schmitt et al., 2017). Namun, implementasi prinsip ini di lapangan masih sulit karena sulitnya menentukan aktor pelaku (attribution problem) dan kompleksitas teknologi yang digunakan dalam serangan siber. Hal ini menjadi tantangan utama bagi negara-negara dalam menegakkan hukum internasional secara efektif di dunia maya.

Temuan lain menunjukkan bahwa konsep kedaulatan siber tidak hanya menyangkut aspek pertahanan dan keamanan, tetapi juga berdampak pada kebebasan berekspresi dan hak privasi individu. Beberapa negara menggunakan dalih kedaulatan digital untuk membatasi akses informasi dan mengontrol aktivitas warganya di dunia maya. Hal ini menimbulkan konflik antara kepentingan keamanan nasional dan perlindungan hak asasi manusia sebagaimana diatur dalam Deklarasi Universal Hak Asasi Manusia (Article 19). Menurut DeNardis (2020), keseimbangan antara keamanan digital dan kebebasan sipil menjadi tantangan besar bagi hukum internasional modern dalam mengatur tata kelola siber global.

Lebih lanjut, munculnya konsep “cyber deterrence” atau pencegahan siber menjadi strategi baru dalam menjaga kedaulatan digital. Negara-negara seperti Amerika Serikat, Rusia, dan Tiongkok mengembangkan kebijakan pertahanan siber yang bersifat ofensif maupun defensif untuk melindungi infrastruktur penting mereka (Lindsay, 2015). Strategi ini seringkali menimbulkan ketegangan geopolitik baru karena melibatkan potensi pelanggaran hukum internasional, terutama jika tindakan pencegahan dilakukan di luar yurisdiksi negara sendiri. Oleh karena itu, diperlukan transparansi dan koordinasi multilateral dalam merumuskan kebijakan keamanan siber global yang sesuai dengan prinsip hukum internasional.

Dalam konteks regional, organisasi seperti ASEAN dan Uni Eropa telah mengambil langkah-langkah untuk membentuk norma bersama dalam penanganan isu kedaulatan siber. ASEAN melalui ASEAN Digital Masterplan 2025 mendorong kolaborasi negara-negara anggotanya dalam memperkuat keamanan siber dan membangun kapasitas hukum yang harmonis (ASEAN Secretariat, 2021). Sementara itu, Uni Eropa

menerapkan EU Cybersecurity Act yang bertujuan meningkatkan standar keamanan digital serta mengatur tanggung jawab negara anggota terhadap insiden siber lintas batas. Upaya ini menunjukkan pentingnya pendekatan kolektif dalam menjaga kedaulatan dan stabilitas siber di tingkat internasional.

Namun demikian, masih terdapat perdebatan di kalangan ahli hukum internasional mengenai sejauh mana prinsip non-intervensi dapat diterapkan dalam ruang siber. Beberapa pakar berpendapat bahwa tindakan siber yang bersifat spionase atau propaganda tidak dapat dikategorikan sebagai pelanggaran kedaulatan karena tidak menimbulkan kerusakan langsung (Tikk & Kaska, 2019). Pandangan ini berbeda dengan kelompok lain yang menilai bahwa setiap intervensi digital tanpa izin merupakan bentuk pelanggaran terhadap integritas negara. Perbedaan tafsir ini menunjukkan perlunya harmonisasi dan pembaruan norma hukum internasional agar mampu menjawab kompleksitas hubungan antarnegara di dunia siber.

Hasil penelitian ini menegaskan bahwa pembentukan norma hukum internasional baru yang secara khusus mengatur aktivitas siber merupakan kebutuhan mendesak. Tanpa adanya regulasi yang jelas, ruang siber berpotensi menjadi arena konflik baru yang sulit dikendalikan. Menurut Nye (2017), penguatan diplomasi digital dan pembentukan perjanjian multilateral tentang keamanan siber global dapat menjadi solusi dalam menciptakan stabilitas jangka panjang. Hukum internasional harus mampu beradaptasi terhadap realitas baru di mana kekuasaan, data, dan informasi menjadi instrumen utama dalam mempertahankan kedaulatan negara.

Akhirnya, tantangan utama hukum internasional modern adalah menyeimbangkan antara perlindungan kedaulatan negara dan pemeliharaan tatanan global yang terbuka dan aman. Kedaulatan siber tidak dapat dipandang secara sempit sebagai hak kontrol negara, tetapi juga sebagai tanggung jawab untuk melindungi hak-hak digital warga negara dan mencegah penyalahgunaan kekuasaan. Kolaborasi internasional yang didukung oleh norma hukum yang kuat menjadi kunci dalam memastikan bahwa ruang siber dapat berfungsi sebagai sarana kemajuan, bukan sumber ancaman bagi perdamaian dan keamanan dunia (Kello, 2017).

KESIMPULAN

Penelitian ini menegaskan bahwa perkembangan teknologi digital dan perluasan ruang siber telah menantang konsep tradisional tentang kedaulatan negara sebagaimana diatur dalam hukum internasional. Dalam dunia tanpa batas fisik seperti ruang siber, kedaulatan tidak lagi terbatas pada wilayah teritorial, melainkan meluas ke pengendalian atas data, jaringan, dan aktivitas digital yang terjadi di dalam yurisdiksi suatu negara. Namun demikian, hingga saat ini belum terdapat instrumen hukum internasional yang secara eksplisit mengatur kedaulatan siber. Prinsip-prinsip umum yang tercantum dalam Piagam PBB masih dijadikan dasar oleh negara-negara dalam menafsirkan hak dan kewajibannya di dunia digital. Hal ini menciptakan ambiguitas yang dapat menimbulkan konflik kepentingan dan ketegangan antarnegara, terutama ketika terjadi pelanggaran melalui serangan siber lintas batas (Schmitt, 2017).

Selanjutnya, penerapan prinsip kedaulatan siber memunculkan dilema antara kebutuhan negara untuk menjaga keamanan nasional dan kewajiban untuk menghormati hak asasi manusia di ruang digital. Dalam banyak kasus, negara menggunakan dalih keamanan siber untuk membenarkan tindakan pengawasan atau pembatasan terhadap kebebasan berekspresi dan privasi warganya. Fenomena ini memperlihatkan bahwa kedaulatan siber memiliki dua sisi: di satu sisi merupakan bentuk perlindungan terhadap ancaman digital, namun di sisi lain berpotensi digunakan sebagai alat kontrol politik (DeNardis, 2020). Oleh karena itu, diperlukan keseimbangan antara perlindungan kepentingan negara dan penghormatan terhadap nilai-nilai universal yang dijamin oleh hukum internasional.

Dari hasil penelitian juga terlihat bahwa upaya kolektif antarnegara menjadi faktor kunci dalam membangun tatanan hukum siber yang stabil dan adil. Inisiatif seperti Tallinn Manual 2.0 dan kebijakan

regional, misalnya ASEAN Digital Masterplan 2025, merupakan langkah awal yang positif dalam merumuskan norma bersama untuk menghadapi ancaman siber global (ASEAN Secretariat, 2021). Namun, efektivitas norma-norma ini masih terbatas karena sifatnya yang tidak mengikat secara hukum (non-binding). Dalam konteks ini, diplomasi siber dan perjanjian multilateral perlu diperkuat agar prinsip-prinsip hukum internasional dapat diterapkan secara lebih konsisten di ruang digital. Dengan adanya kerangka hukum yang lebih jelas, negara-negara dapat menegakkan kedaulatannya tanpa menimbulkan konflik yang melanggar prinsip non-intervensi.

Akhirnya, penelitian ini menegaskan pentingnya pembentukan norma hukum internasional baru yang spesifik mengatur aktivitas siber, termasuk penentuan batas yurisdiksi, tanggung jawab negara atas serangan digital, serta mekanisme penyelesaian sengketa siber. Dunia siber tidak dapat diatur dengan paradigma hukum tradisional yang hanya berfokus pada wilayah fisik. Dibutuhkan pendekatan hukum yang lebih dinamis, adaptif, dan kolaboratif agar ruang siber dapat menjadi ekosistem global yang aman, adil, dan menghormati prinsip-prinsip kedaulatan serta hak asasi manusia. Dengan demikian, hukum internasional modern dituntut untuk bertransformasi seiring perkembangan teknologi agar tetap relevan dalam menjaga perdamaian dan stabilitas global di era digital (Nye, 2017; Kello, 2017).

DAFTAR PUSTAKA

ASEAN Secretariat. (2021). ASEAN Digital Masterplan 2025. Jakarta: ASEAN.

Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.

Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.

DeNardis, L. (2020). *The Internet in Everything: Freedom and Security in a World with No Off Switch*. Yale University Press.

Kello, L. (2017). The Virtual Weapon and International Order. Yale University Press.

Kleffner, J. K. (2013). The applicability of the law of armed conflict to cyber operations. International Law Studies, 89(1), 45–67.

Krasner, S. D. (2020). Sovereignty: Organized Hypocrisy Revisited. International Theory, 12(1), 1–25. https://doi.org/10.1017/S1752971919000235

Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. International Security, 40(3), 7–47.

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. International Security, 41(3), 44–71.

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Tikk, E., & Kaska, K. (2019). *International Cyber Norms and the Sovereignty Debate*. *Journal of Cyber Policy*, 4(1), 1–20. https://doi.org/10.1080/23738871.2019.1604785

Tsagourias, N., & Buchan, R. (2015). Cyber interventions and international law. Cambridge University Press.