**Arus Jurnal Sosial dan Humaniora (AJSH)**
*Website: http://jurnal.ardenjaya.com/index.php/ajsh*
*Email: jurnal.ajsh@ardenjaya.com*

# Analisis Normatif Hukum Internasional dan Kesiapan Regulasi Indonesia Menghadapi Ancaman *Cyberwarfare* Lintas Batas

**INFO PENULIS**

Rania Aisya Saudira
Universitas Pelita Harapan
raniasaudira922@gmail.com

**INFO ARTIKEL**

ISSN: 2808-1307
Vol. 5, No. 3, Desember 2025
https://jurnal.ardenjaya.com/index.php/ajsh



***Saran Penulisan Referensi:***

Saudira, R. A. (2025). Analisis Normatif Hukum Internasional dan Kesiapan Regulasi Indonesia Menghadapi Ancaman Cyberwarfare Lintas Batas. *Arus Jurnal Sosial dan Humaniora, 5* (3),4008-4014.

**Abstrak**

Penelitian ini bertujuan untuk menganalisis tantangan penerapan hukum internasional terhadap praktik *cyberwarfare* serta meninjau kesiapan regulasi nasional Indonesia dalam menghadapi ancaman tersebut. Metode penelitian yang digunakan adalah pendekatan hukum normatif dengan menelaah berbagai literatur, instrumen hukum internasional, dan kebijakan nasional yang relevan. Hasil penelitian menunjukkan bahwa hukum internasional belum memiliki instrumen khusus yang mengatur perang siber secara komprehensif. Prinsip-prinsip umum seperti kedaulatan negara, tanggung jawab negara, dan larangan penggunaan kekuatan masih dijadikan dasar interpretasi dalam menilai legalitas tindakan *cyberwarfare*. Di Indonesia, kerangka hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peran BSSN menunjukkan upaya mitigasi terhadap ancaman siber, namun belum mencakup aspek pertahanan digital secara menyeluruh. Kesimpulannya, diperlukan harmonisasi antara hukum nasional dan hukum internasional, serta pembentukan norma global baru yang mampu menjawab tantangan perang siber di era digital.

**Kata Kunci :** *Cyberwarfare*, Hukum Internasional, Informasi Transaksi Elektronik, Keamanan Digital, Teknologi Digital

**Abstract**

This study aims to analyze the challenges of applying international law to cyberwarfare practices and review Indonesia's national regulatory readiness to address these threats. The research method used is a normative legal approach by examining various literature, international legal instruments, and relevant national policies. The results show that international law does not yet have a specific instrument that comprehensively regulates cyberwarfare. General principles such as state sovereignty, state responsibility, and the prohibition on the use of force are still used as the basis for interpretation in assessing the legality of cyberwarfare actions. In Indonesia, legal frameworks such as the Electronic Information and Transactions Law (UU ITE) and the role of the National Cyber and Cyber Security Agency (BSSN) demonstrate efforts to mitigate cyber threats, but do not yet fully encompass aspects of digital defense. In conclusion, harmonization of national and international law is needed, as well as the establishment of new global norms capable of addressing the challenges of cyberwarfare in the digital era.

**Keywords:** Cyberwarfare, International Law, Electronic Transaction Information, Digital Security, Digital Technology

## A. Pendahuluan

Perang siber (*cyberwarfare*) merupakan fenomena baru yang lahir dari kemajuan pesat teknologi digital dan kini menjadi salah satu tantangan terbesar bagi kerangka hukum internasional modern. Berbeda dengan bentuk peperangan konvensional yang mengandalkan kekuatan fisik dan senjata kinetik, perang siber berlangsung di ruang maya yang tak berbatas, melibatkan serangan terhadap jaringan komputer, sistem pertahanan, hingga infrastruktur vital seperti energi, transportasi, komunikasi, dan perbankan (Ariyaningsih *et al*., 2023). Serangan semacam ini dapat dilancarkan tanpa perlu kehadiran pasukan di medan perang, namun dampaknya dapat melumpuhkan fungsi pemerintahan dan mengancam stabilitas suatu negara dalam hitungan detik. Dengan kata lain, *cyberwarfare* telah mengaburkan batas antara masa damai dan masa perang, antara tindakan kriminal dan agresi militer.

*Cyberwarfare* bukan lagi wacana masa depan, tetapi realitas yang telah menjadi ancaman serius bagi ketahanan nasional. Serangan siber mampu melumpuhkan aspek vital seperti ekonomi dan komunikasi tanpa memerlukan peluru fisik. Ancaman siber ini juga telah menembus batas teritorial dan berpotensi mengguncang stabilitas nasional , menegaskan bahwa isu ini menyangkut aspek hukum, politik, dan kedaulatan negara di dunia maya, bukan sekadar masalah teknologi.

Fenomena ini menimbulkan pertanyaan mendasar bagi hukum internasional tentang sejauh mana norma-norma tradisional yang berbasis pada kekuatan fisik, seperti yang diatur dalam Piagam Perserikatan Bangsa-Bangsa dan Hukum Humaniter Internasional, masih relevan dalam menghadapi serangan yang bersifat digital dan anonimitas. Prinsip-prinsip seperti kedaulatan, non-intervensi, dan tanggung jawab negara kini diuji dalam konteks yang sama sekali baru, di mana pelaku serangan bisa jadi bukan negara, melainkan kelompok non-negara atau bahkan individu dengan kemampuan teknis tinggi.

Tinjauan literatur menunjukkan adanya *legal gap* yang signifikan. Regulasi yang mengatur penggunaan kekuatan di dunia maya masih belum jelas dan cenderung bersifat interpretatif. Para ahli menilai bahwa konsep *cyber attack*, *cyber crime*, dan *cyber warfare* masih tumpang tindih secara yuridis. Hukum internasional belum memiliki instrumen khusus yang mengatur perang siber secara komprehensif. Tidak ada perjanjian internasional yang secara eksplisit mengatur perang siber, sehingga interpretasi hukum banyak bergantung pada dokumen seperti *Tallinn Manual 2.0*. Namun, solusi ini memiliki batasan signifikan, antara lain bersifat *soft law* dan ambigu. Bahkan, Togatorop, Lestarika, dan Sari (2025) menemukan bahwa kejahatan siber belum sepenuhnya dapat dikategorikan sebagai *war crimes* dalam kerangka hukum humaniter internasional.

Kompleksitas atribusi menentukan siapa pelaku dan dari mana serangan berasal, menjadi kendala utama dalam penerapan hukum internasional , yang pada akhirnya menyebabkan lemahnya tanggung jawab hukum dan kesulitan dalam menerapkan sanksi internasional. Pada tingkat nasional, Indonesia juga menghadapi tantangan implementasi. Strategi pertahanan siber tidak dapat dilepaskan dari kerangka hukum internasional, terutama dalam hal tanggung jawab negara atas serangan siber lintas batas (Darumaya et al., 2023). Putri, Pratama, dan Fithri (2023) bahkan menyoroti bahwa Indonesia berada dalam kondisi "darurat siber *warfare*". Meskipun sudah ada kerangka hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan pembentukan Badan Siber dan Sandi Negara (BSSN), penelitian menunjukkan bahwa regulasi nasional masih bersifat fragmentaris dan lebih berfokus pada aspek keamanan informasi dan penegakan hukum terhadap *cybercrime*, bukan pada aspek pertahanan negara dari potensi *cyberwarfare*. Tantangan juga meliputi koordinasi antar-lembaga, kesiapan teknologi, kapasitas sumber daya manusia , serta minimnya sistem deteksi dini. Dengan demikian, *cyberwarfare* bukan hanya isu keamanan teknologi, tetapi juga ujian bagi efektivitas, adaptabilitas, dan relevansi hukum internasional di era digital. Penelitian ini memandang istilah "*cyberwarfare*" sebagai dimensi konflik baru yang memerlukan analisis normatif tentang bagaimana hukum internasional menanggapi operasi siber lintas-batas, sekaligus mengkaji efektivitas norma yang ada dalam mencegah atau mengatur serangan siber yang merusak.

Permasalahan yang menjadi fokus penelitian ini adalah sejauh mana hukum internasional mampu mengatur perang siber dan apakah norma yang ada cukup untuk menanggapi operasi siber yang menimbulkan kerusakan atau ancaman terhadap infrastruktur kritikal. *Gap* penelitian yang ingin diisi oleh studi ini adalah pengembangan kerangka normatif yang lebih jelas, adaptif, dan aplikatif terhadap konflik siber, termasuk definisi *use of force*, tanggung jawab negara, dan perlindungan infrastruktur kritikal.

Penelitian ini berupaya mengisi kesenjangan yang ada dengan menawarkan sebuah kerangka regulasi normatif yang tidak hanya konseptual, tetapi juga aplikatif terhadap dinamika nyata perang siber. Kontribusi utama dari penelitian ini terletak pada tiga aspek penting. Pertama, memberikan pemahaman sistematis tentang bagaimana hukum internasional merespons fenomena perang siber. Kedua, menyusun kerangka regulasi normatif yang adaptif. Ketiga, menawarkan rekomendasi konkret bagi komunitas internasional untuk memperjelas mekanisme atribusi dan tanggung jawab negara. Penelitian ini diharapkan menghasilkan dua temuan utama yaitu meningkatnya kepastian hukum dan akuntabilitas dalam penyelesaian konflik siber, dan penguatan norma tanggung jawab negara dan kejelasan mekanisme atribusi yang mampu menekan frekuensi serta eskalasi operasi siber antarnegara.

## B. Metodologi

Penelitian ini meneliti penerapan dan tantangan *cyberwarfare* dalam perspektif hukum internasional dengan fokus pada tanggung jawab negara dan kedaulatan digital. Penelitian dilakukan melalui studi kepustakaan (*library research*) yang bersifat nonfisik, dengan karakteristik lokasi penelitian berpusat pada sumber-sumber hukum dan literatur ilmiah yang relevan. Sumber data terdiri dari bahan hukum primer, serta bahan hukum sekunder berupa buku, jurnal, dan artikel ilmiah dari peneliti nasional maupun internasional.

Populasi penelitian mencakup literatur hukum yang membahas isu perang siber dalam kurun waktu lima tahun terakhir, dengan teknik pengambilan sampel menggunakan *purposive sampling*, yaitu pemilihan sumber data berdasarkan pertimbangan relevansi dan kredibilitasnya terhadap masalah penelitian (Sugiyono, 2022). Data diperoleh melalui penelusuran sistematis terhadap basis data ilmiah dan dokumen hukum, kemudian dianalisis menggunakan metode kualitatif deskriptif. Variabel penelitian diukur berdasarkan kesesuaian norma hukum internasional dengan praktik *cyberwarfare* serta implikasinya terhadap kebijakan nasional. Analisis dilakukan dengan pendekatan deduktif, yakni menarik kesimpulan dari teori umum menuju kasus konkret (Arikunto, 2021).

Karena penelitian ini bersifat kualitatif normatif, tidak digunakan prosedur statistik dalam pengolahan data. Tantangan utama yang dihadapi adalah keterbatasan literatur yang secara spesifik membahas perang siber dalam konteks hukum internasional, sementara keunggulan metode ini terletak pada kemampuannya memberikan pemahaman mendalam dan argumentatif terhadap norma hukum yang berlaku serta relevansinya dengan dinamika keamanan siber global.

## C. Hasil dan Pembahasan

1. Hasil

Guna mendukung analisis dalam penelitian ini, penulis menelaah beberapa artikel jurnal dari peneliti Indonesia yang relevan dengan tema cyberwarfare dan implikasinya terhadap hukum internasional maupun keamanan nasional. Kajian ini bertujuan untuk memberikan gambaran mengenai perkembangan penelitian terkini di Indonesia terkait perang siber, baik dari sisi konsep, regulasi, maupun strategi penanganannya.

Tabel 1. Penelitian Terkait

| Penulis (tahun) | Judul | Tujuan | Metode | Hasil |
|---|---|---|---|---|
| Yanuar, A. P . (2021) | Cyber war: Ancaman Baru Keamanan Nasional dan Internasional | Menganalisis ancaman perang siber (cyber war) pada skala internasional dan dampaknya masa depan. | Metode campuran (kualitatif + kuantitatif) dengan studi literatur dan data sekunder. | Ancaman perang siber sudah nyata dan harus diperhitungkan dalam keamanan nasional/internasional; negara perlu konsep keamanan siber yang |

| Penulis (tahun) | Judul | Tujuan | Metode | Hasil |
|---|---|---|---|---|
| | | | | matang. |
| Suharto, M. A. (2021) | Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional | Membahas definisi dan perbedaan antara cyber attack, cyber crime, dan cyber warfare serta relevansinya regulasi internasional | Penelitian normatif/doktrinal dengan studi literatur. | Ditemukan bahwa banyak tumpang-tindih konsep dan regulasi internasional belum spesifik mengatur perang siber; perlunya klarifikasi definisi. |
| Togatorop, F. M., Lestarika, D. P., & Sari, W. (2025) | Analisis Kejahatan Siber Sebagai Kejahatan Perang Berdasarkan Hukum Humaniter Internasional | Mengkaji apakah kejahatan siber bisa dikategorikan sebagai kejahatan perang menurut hukum humaniter internasional | Pendekatan normatif-yuridis dengan analisis literatur dan regulasi internasional. | Kesimpulan bahwa regulasi saat ini belum memadai untuk menampung perang siber secara eksplisit; rekomendasi pengembangan payung hukum baru. |
| Putri, E., Pratama, G. A., & Fithri, B. S. (2023) | Keamanan Nasional dalam Menghadapi Perubahan Cyber Warfare | Menggambarkan kondisi dan tantangan strategi keamanan nasional Indonesia dalam menghadapi perang siber | Penelitian kualitatif deskriptif dengan studi pustaka atau sekunder. | Ditemukan bahwa Indonesia dalam kondisi “darurat siber warfare”; rekomendasi penguatan regulasi, SDM, dan kerjasama |
| Santoso, F. B., Pujianto, R., & Ramadhan, T. (2024) | Smishing Guard: Strategi Pengembangan Sistem Deteksi Dan Respons Ancaman Sms Phishing | Menganalisis ancaman keamanan siber di Asia Tenggara dan strategi Indonesia dalam penanganannya | Studi literatur atau sekunder dengan pendekatan kualitatif. | Menemukan bahwa ketidakseimbangan kapasitas teknologi antar-negara ASEAN menjadi kerentanan, dan Indonesia butuh kerja sama multinasional dan penguatan nasional. |

2. Pembahasan

Perkembangan teknologi informasi telah mengubah wajah konflik modern. Jika dahulu perang hanya terjadi melalui kekuatan militer konvensional, kini serangan dapat dilakukan tanpa peluru, melalui ruang siber. Menurut Yanuar (2021), *cyberwarfare* merupakan ancaman keamanan baru yang berpotensi menimbulkan kerusakan strategis terhadap infrastruktur vital suatu negara. Ia menegaskan bahwa perang siber bukan lagi wacana masa depan, tetapi realitas yang tengah dihadapi banyak negara, termasuk Indonesia. Serangan siber terhadap fasilitas pemerintah dan lembaga strategis membuktikan bahwa kedaulatan suatu negara kini tak hanya diukur dari pertahanan teritorial, tetapi juga kemampuan mengamankan sistem informasinya.

Selain itu, Putri, Pratama, dan Fithri (2023) menyoroti bahwa konsep keamanan nasional kini harus menyesuaikan diri dengan dinamika *cyberwarfare*. Indonesia masih berada pada tahap "darurat siber", di mana ancaman datang tidak hanya dari luar, tetapi juga dari dalam negeri melalui peretasan, propaganda digital, dan penyebaran disinformasi. Situasi ini menuntut kebijakan hukum dan strategi keamanan nasional yang adaptif terhadap ancaman digital lintas batas.

Dalam tataran hukum internasional, prinsip kedaulatan dan tanggung jawab negara menjadi pijakan utama dalam menilai legalitas perang siber. Suharto (2021) menjelaskan bahwa konsep *cyber attack*, *cyber crime*, dan *cyber warfare* masih tumpang tindih secara yuridis. Tidak ada perjanjian internasional yang secara eksplisit mengatur perang siber, sehingga interpretasi hukum banyak bergantung pada *Tallinn Manual 2.0*. Prinsip larangan penggunaan kekuatan bersenjata sering kali dijadikan dasar untuk menilai legalitas serangan siber, meskipun penerapannya masih menimbulkan perdebatan, terutama dalam hal pembuktian keterlibatan negara (*attribution*).

Togatorop, Lestarika, dan Sari (2025) memperkuat pandangan tersebut dengan menilai bahwa kejahatan siber belum sepenuhnya dapat dikategorikan sebagai *war crimes* dalam kerangka hukum humaniter internasional. Mereka menemukan adanya kekosongan norma (*legal gap*) yang membuat perang siber sulit diadili di ranah internasional, terutama ketika serangan siber tidak menimbulkan korban jiwa secara langsung. Oleh karena itu, perlu adanya pembaruan hukum internasional yang secara khusus mengatur bentuk-bentuk konflik digital.

Tantangan utama dalam penerapan hukum internasional terhadap perang siber adalah masalah atribusi dan yurisdiksi. Seperti dijelaskan oleh Yanuar (2021), sulit bagi komunitas internasional untuk menentukan pelaku serangan siber karena serangan tersebut sering kali dilakukan secara anonim dan lintas negara. Hal ini menyebabkan lemahnya tanggung jawab hukum dan kesulitan dalam menerapkan sanksi internasional.

Di tingkat nasional, Putri et al. (2023) dan Santoso, Pujianto, serta Ramadhan (2024) mencatat bahwa regulasi Indonesia belum sepenuhnya mampu menjawab kompleksitas *cyberwarfare*. Meskipun sudah ada UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) dan pembentukan Badan Siber dan Sandi Negara (BSSN), implementasinya masih lemah dalam aspek koordinasi antarlembaga dan kesiapsiagaan sumber daya manusia. Dalam konteks ASEAN, Indonesia juga menghadapi tantangan ketimpangan kemampuan teknologi, yang menyebabkan kerentanan kolektif terhadap serangan siber lintas negara.

Hasil kajian terhadap kelima artikel menunjukkan adanya kesenjangan yang cukup besar antara prinsip hukum internasional dan kebijakan nasional dalam menghadapi fenomena *cyberwarfare*. Di satu sisi, hukum internasional masih berjuang untuk merumuskan kerangka regulasi yang mampu mengakomodasi karakter non-fisik, anonim, dan lintas batas dari perang siber. Kompleksitas ini muncul karena sulitnya menentukan pelaku, motif, dan lokasi serangan, yang pada akhirnya menyulitkan penerapan prinsip tanggung jawab negara. Meskipun dokumen seperti *Tallinn Manual 2.0* telah berupaya memberikan pedoman interpretatif terhadap penerapan hukum internasional di ranah siber, sifatnya masih bersifat *non-binding* dan belum memiliki kekuatan hukum yang mengikat negara-negara anggota Perserikatan Bangsa-Bangsa. Akibatnya, setiap negara menafsirkan tindakan siber berdasarkan kepentingan nasional masing-masing, yang justru memperlebar kesenjangan antara prinsip universal dan praktik di lapangan.

Sementara itu, di sisi hukum nasional Indonesia, kebijakan dan regulasi yang ada seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta pembentukan Badan Siber dan Sandi Negara (BSSN), menunjukkan langkah positif dalam memperkuat ketahanan digital nasional. Namun, kerangka hukum ini belum sepenuhnya memposisikan ancaman siber sebagai bagian dari rezim hukum pertahanan negara. Fokus kebijakan Indonesia masih berkisar pada aspek keamanan informasi dan penegakan hukum terhadap kejahatan siber (*cybercrime*), bukan terhadap serangan siber yang berpotensi

bersifat militer atau strategis. Hal ini menimbulkan celah dalam tata kelola pertahanan siber yang terintegrasi antara lembaga sipil dan militer.

Secara normatif, prinsip kedaulatan negara dalam hukum internasional seharusnya dapat diadaptasi untuk melindungi kedaulatan ruang digital suatu negara. Namun demikian, dibutuhkan kejelasan batasan antara serangan siber yang hanya menimbulkan gangguan teknis ringan dengan serangan yang dapat dikategorikan sebagai tindakan agresi dalam kerangka *jus ad bellum*. Tanpa kejelasan ini, negara akan kesulitan menentukan kapan mereka memiliki hak untuk melakukan tindakan pembelaan diri (*self-defense*) di dunia maya. Oleh karena itu, Indonesia memiliki peluang strategis untuk mengambil peran aktif dalam diplomasi hukum internasional, khususnya di forum seperti ASEAN, ITU, dan PBB, guna mendorong pembentukan norma-norma hukum baru mengenai *cyberwarfare*. Norma tersebut idealnya bersifat komprehensif, inklusif terhadap kepentingan negara berkembang, dan mampu menyeimbangkan antara aspek keamanan, kedaulatan digital, serta hak asasi manusia di era digital.

Dari hasil pembahasan terhadap kelima artikel yang dikaji, dapat diidentifikasi sejumlah temuan penting yang mencerminkan kompleksitas isu *cyberwarfare* dalam konteks hukum dan kebijakan publik. *Cyberwarfare* muncul sebagai bentuk ancaman modern yang tidak hanya berdampak pada aspek teknis atau infrastruktur digital, tetapi juga secara langsung mengancam kedaulatan dan keamanan nasional. Serangan siber yang menargetkan sistem pemerintahan, militer, dan sektor vital lainnya mampu melemahkan stabilitas negara tanpa perlu melalui konflik bersenjata konvensional. Hal ini menandakan bahwa perang di era digital tidak lagi terbatas pada ranah fisik, melainkan telah meluas menjadi perang informasi dan data.

Hasil kajian menunjukkan belum adanya instrumen hukum internasional yang secara eksplisit mengatur tentang perang siber. Kerangka hukum yang ada saat ini masih bergantung pada prinsip umum seperti larangan penggunaan kekuatan bersenjata (*prohibition of the use of force*) dan tanggung jawab negara (*state responsibility*). Dokumen interpretatif seperti *Tallinn Manual 2.0* memang memberikan panduan awal dalam mengaplikasikan hukum internasional terhadap dunia maya, namun karena sifatnya *non-binding*, implementasinya bergantung pada kesediaan dan kepentingan masing-masing negara. Akibatnya, muncul ketimpangan penafsiran dan penerapan norma hukum di tingkat global.

Di level nasional, Indonesia telah menunjukkan langkah maju melalui pembentukan Badan Siber dan Sandi Negara (BSSN), penerapan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta sejumlah kebijakan keamanan digital. Namun demikian, penelitian-penelitian tersebut sepakat bahwa regulasi nasional Indonesia masih bersifat fragmentaris dan lebih berfokus pada aspek keamanan informasi serta penegakan hukum terhadap kejahatan siber, bukan pada aspek pertahanan negara dari potensi *cyberwarfare*. Masih diperlukan koordinasi lintas sektor antara lembaga pertahanan, komunikasi, dan intelijen agar sistem pertahanan siber Indonesia mampu bekerja secara terpadu dan responsif terhadap ancaman lintas batas.

Pendekatan normatif yang digunakan dalam penelitian ini menegaskan urgensi sinkronisasi antara hukum internasional dan hukum nasional. Kesenjangan di antara keduanya menciptakan ruang abu-abu dalam penegakan hukum dan kebijakan pertahanan siber. Indonesia dapat mengambil posisi strategis dalam diplomasi internasional untuk mendorong pembentukan norma global baru yang mengatur perang siber secara komprehensif dan inklusif terhadap kepentingan negara berkembang. Dengan langkah tersebut, diharapkan lahir tatanan hukum siber yang tidak hanya melindungi kepentingan nasional, tetapi juga memperkuat solidaritas global dalam menjaga stabilitas dan perdamaian dunia di era digital.

## D. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa cyberwarfare merupakan bentuk konflik modern yang menimbulkan tantangan serius bagi tatanan hukum internasional dan nasional. Meskipun prinsip-prinsip dasar seperti kedaulatan, tanggung jawab negara, dan larangan penggunaan kekuatan bersenjata masih menjadi acuan utama, belum ada instrumen hukum internasional yang secara spesifik mengatur perang siber, sehingga aspek atribusi dan pembuktian pelaku menjadi kendala utama. Di Indonesia, regulasi seperti UU ITE dan keberadaan BSSN menunjukkan langkah positif dalam menghadapi ancaman siber, namun masih bersifat reaktif dan belum terintegrasi dalam sistem pertahanan negara yang komprehensif. Oleh karena itu, diperlukan pembaruan regulasi, peningkatan kapasitas sumber daya manusia, serta upaya diplomasi hukum internasional untuk mendorong terbentuknya norma global yang mengatur cyberwarfare secara lebih jelas dan adil.

## E. Referensi


Ahmad, K., Sajid, F., & Bourkrain, W. (2024). Cyberwarfare: Exploring the inadequacies of classical international humanitarian law. *UCP Journal of Law & Legal Education*, *2*(1), 28–57. https://doi.org/10.24312/ucp-jlle.02.01.159

Arikunto, S. (2021). *Prosedur penelitian: Suatu Pendekatan Praktik (Edisi Revisi)*. Rineka Cipta.

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1-11. https://doi.org/10.56457/jjih.v1i1.38

Babys, S. A. M. (2021). Ancaman Perang Siber di Era Digital dan Solusi Keamanan Indonesia. *Jurnal Oratio Directa*, *3*(1), 425–442.

Bhaiyat, H., & Sithungu, S. (2022). Cyberwarfare and Its Effects on Critical Infrastructure. *International Conference on Cyber Warfare and Security*, *17*(1), 536–543. https://doi.org/10.34190/iccws.17.1.68

Buchan, R., & Tsagourias, N. (2024). Cyberwarfare and International Law. Dalam *Research handbook on cyberwarfare*. Edward Elgar Publishing. https://doi.org/10.4337/9781803924854.00028

Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan (*Thoughts on the Potential Threat of Cyber War in Indonesia: A Defense Strategy Study*). *Jurnal Keamanan Nasional*, *9*(2), 299–324. https://ejurnal.ubharajaya.ac.id/index.php/kamnas

Haataja, S. (2022). Cyber Operations Against Critical Infrastructure Under Norms of Responsible State Behaviour and International Law. *International Journal of Law and Information Technology*, *30*(4), 423–443. https://doi.org/10.1093/ijlit/eaad006

Krisnata, R., Reksoprodjo, A. H. S., & Waluyo, S. D. (2022). Strategi Pengembangan Kapabilitas Siber Pertahanan untuk Menghadapi Peperangan Siber (Studi Kasus Pada PUSHANSIBER KEMHAN RI 2020-2021). *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *9*(6).

Putri, E., Pratama, G. A., & Fithri, B. S. (2023). Keamanan Nasional dalam Menghadapi Perubahan Cyber Warfare. *JURNAL MERCATORIA*, *16*(2), 201–208. https://doi.org/10.31289/mercatoria.v16i2.9534

Rosli, W. R. W. (2025). Waging Warfare Against States: The Deployment of Artificial Intelligence in Cyber Espionage. *AI and Ethics*, *5*(1), 47–53. https://doi.org/10.1007/s43681-024-00628-x

Santoso, F. B., Pujianto, R., & Ramadhan, T. (2024). Smishing Guard: Strategi Pengembangan Sistem Deteksi dan Respons Ancaman SMS Phishing. *Journal of Information and Information Security (JIFORTY)*, *5*(2). http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Sugiyono. (2022). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare dalam Aspek Hukum Internasional. *Risalah Hukum*, *17*, 98–107. https://doi.org/10.30872/risalah.v17i2.705

Togatorop, F. M., Lestarika, D. P., & Sary, W. E. (2025). Analisis Kejahatan Siber Sebagai Kejahatan Perang Berdasarkan Hukum Humaniter Internasional. *Jurnal Kajian Hukum, 1*(3), 256–261. https://jurnal.globalscients.com/index.php/jkhpk/article/view/417

Yanuar, A. P. (2021). Cyber War: Ancaman Baru Keamanan Nasional dan Internasional. *Jurnal Keamanan Nasional*, *7*(1), 23–35. https://doi.org/10.31599/jkn.v7i1.474