Journal of Law, Administration, and Social Science
Volume 5 No.4, 2025

TANGGUNG JAWAB NEGARA MENURUT UUD 1945 TERHADAP ANCAMAN SIBER DAN PERANG HIBRIDA

Wilma Silalahi [1]; Gesta Subysesa Maharwani Adeputri [2]

[1] wilmasilalahi@fh.untar.ac.id, *Universitas Tarumanagara*
[2] subsesamaharwani@gmail.com *Universitas Tarumanagara*

Abstract
The rapid development of digital technology and global geopolitical dynamics has given rise to new threats in the form of cyberattacks and hybrid warfare, challenging Indonesia's national resilience. These threats are not limited to military aggression but also include non-military dimensions such as data breaches, ransomware attacks, and political disinformation. This study aims to analyze the state's responsibility under the 1945 Constitution of the Republic of Indonesia in addressing cyber threats and hybrid warfare, while also evaluating the adequacy of the current national legal framework. This research employs normative legal methods with statutory and conceptual approaches. The findings indicate that Article 30 of the 1945 Constitution affirms the state as the primary actor in ensuring national defense and security. However, existing laws—such as Law No. 3 of 2002 on National Defense, Law No. 34 of 2004 on the Indonesian Armed Forces, and the Electronic Information and Transactions Law—remain oriented toward conventional threats, leaving legal gaps in addressing hybrid warfare. Therefore, a comprehensive and adaptive cyber defense policy is urgently required to respond effectively to contemporary challenges.
Keywords: *1945 Constitution; Cyber threats; Hybrid warfare; National defense; State responsibility*

Abstrak
Perkembangan teknologi digital dan dinamika geopolitik global telah melahirkan ancaman baru berupa serangan siber dan perang hibrida yang menguji ketahanan nasional Indonesia. Ancaman ini tidak hanya bersifat militer, tetapi juga non-militer melalui kebocoran data, serangan ransomware, serta disinformasi politik. Penelitian ini bertujuan untuk menganalisis bentuk tanggung jawab negara menurut UUD 1945 dalam menghadapi ancaman siber dan perang hibrida, sekaligus menilai kecukupan kerangka hukum nasional yang berlaku. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Hasil kajian menunjukkan bahwa Pasal 30 UUD 1945 menegaskan negara sebagai aktor utama dalam menjamin pertahanan dan keamanan nasional, namun regulasi positif di Indonesia, seperti UU No. 3 Tahun 2002 tentang Pertahanan Negara, UU No. 34 Tahun 2004 tentang TNI, dan UU ITE, masih lebih berorientasi pada ancaman konvensional. Hal ini menimbulkan celah hukum dalam menghadapi kompleksitas ancaman hibrida. Oleh karena itu, diperlukan pembaruan kebijakan pertahanan siber nasional yang lebih adaptif, integratif, dan sesuai dengan dinamika ancaman kontemporer.
Kata Kunci: Ancaman siber; Perang hibrida; Pertahanan nasional; Tanggung jawab negara; UUD 1945

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa dampak signifikan terhadap dinamika sosial, ekonomi, politik, dan pertahanan suatu negara. Transformasi digital tidak hanya membuka peluang pembangunan nasional, tetapi juga menghadirkan ancaman baru yang bersifat non-tradisional. Ancaman tersebut mencakup serangan siber, disinformasi, propaganda politik, dan tekanan ekonomi yang menjadi bagian dari *hybrid warfare* (Rafel, 2023).

Indonesia sebagai negara kepulauan dengan posisi strategis di kawasan Indo-Pasifik memiliki tingkat kerentanan yang tinggi terhadap ancaman ini. Kasus kebocoran data pribadi, serangan ransomware terhadap sistem pemerintahan, serta maraknya disinformasi politik menjelang pemilu menjadi bukti bahwa ancaman hibrida nyata dan dapat mengganggu stabilitas negara. Kondisi tersebut menuntut negara memiliki kerangka hukum dan kebijakan pertahanan yang adaptif untuk menjamin kedaulatan dan keamanan nasional (To, 2025).

Dalam perspektif hukum tata negara, UUD 1945 menegaskan bahwa pertahanan dan keamanan negara merupakan tanggung jawab bersama seluruh warga negara, dengan negara

sebagai aktor utama dalam menjamin kedaulatan bangsa. Pasal 30 UUD 1945 secara eksplisit mengatur sistem pertahanan dan keamanan rakyat semesta (Sishankamrata), yang menempatkan negara pada posisi sentral dalam menghadapi ancaman terhadap kedaulatan nasional. Namun, kerangka hukum yang ada—seperti UU No. 3 Tahun 2002 tentang Pertahanan Negara, UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia, dan UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik—masih berorientasi pada ancaman konvensional. Hal ini menimbulkan pertanyaan sejauh mana regulasi tersebut memadai dalam menghadapi ancaman hibrida yang bersifat multidimensional.(Supriyadi, 2025)

Kajian sebelumnya menunjukkan bahwa regulasi pertahanan dan keamanan siber di Indonesia masih parsial dan belum sepenuhnya terintegrasi antar-lembaga. Hal ini berbeda dengan praktik di negara-negara maju yang telah mengembangkan strategi pertahanan hibrida secara komprehensif, dengan melibatkan koordinasi lintas sektor dan pendekatan multidimensi. (Pramono & Pertahanan, 2025)Dengan demikian, kajian mengenai tanggung jawab negara menurut UUD 1945 dalam menghadapi ancaman siber dan perang hibrida penting dilakukan untuk memperkuat landasan akademik sekaligus memberikan rekomendasi bagi pembaruan kebijakan pertahanan nasional.

KAJIAN PUSTAKA

Tanggung Jawab Negara Menurut UUD 1945

Dalam hukum tata negara Indonesia, prinsip tanggung jawab negara diatur dalam UUD 1945, khususnya Pasal 30 yang menegaskan bahwa pertahanan dan keamanan negara adalah tanggung jawab bersama warga negara dengan negara sebagai aktor utama. Konsep ini menempatkan negara pada posisi sentral dalam menjamin keberlangsungan kedaulatan, keutuhan wilayah, dan keselamatan bangsa. Prinsip tersebut sejalan dengan doktrin *state responsibility* dalam hukum internasional yang menyatakan bahwa negara memiliki kewajiban untuk melindungi warganya dari ancaman, baik yang berasal dari dalam maupun luar negeri.

Ancaman Siber dan Perang Hibrida

Ancaman siber merupakan bentuk ancaman non-tradisional yang semakin dominan pada era digital. Serangan siber dapat meliputi pencurian data, sabotase sistem informasi, hingga serangan terhadap infrastruktur kritis.(Darumaya et al., 2023) Sementara itu, perang hibrida adalah kombinasi strategi militer dan non-militer, termasuk operasi informasi, propaganda, serta instrumen ekonomi untuk melemahkan stabilitas negara sasaran. Di Indonesia, kasus kebocoran data dan disinformasi politik menjelang pemilu menjadi contoh nyata dari kompleksitas ancaman hibrida yang tidak dapat ditangani dengan pendekatan pertahanan konvensional semata.(Wijanarko et al., 2025)

Kerangka Hukum Nasional dalam Pertahanan dan Keamanan Sejumlah regulasi telah mengatur tentang pertahanan dan keamanan nasional, di antaranya UU No. 3 Tahun 2002 tentang Pertahanan Negara, UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia, serta UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Namun, kajian menunjukkan bahwa regulasi tersebut masih lebih berfokus pada ancaman konvensional dan belum sepenuhnya adaptif terhadap ancaman multidimensi seperti perang hibrida. Keterbatasan tersebut berdampak pada lemahnya koordinasi antar-lembaga, khususnya antara institusi pertahanan, keamanan, dan siber (Pratama, 2022).

Penelitian Terdahulu

Beberapa penelitian telah membahas isu ini menemukan bahwa kebijakan pertahanan Indonesia masih kurang responsif terhadap ancaman siber karena belum adanya strategi nasional yang terintegrasi. Sementara itu, (Maharani et al., 2025) menekankan pentingnya pembaruan doktrin pertahanan nasional agar mampu menjawab tantangan perang hibrida yang

bersifat asimetris. Penelitian lain juga menunjukkan bahwa negara-negara di Eropa dan Asia Timur telah lebih dulu mengadopsi strategi pertahanan siber nasional yang komprehensif, termasuk perlindungan infrastruktur digital dan sistem deteksi dini

Kerangka Pemikiran

Berdasarkan uraian di atas, kerangka pemikiran penelitian ini mengasumsikan bahwa tanggung jawab negara menurut UUD 1945 menjadi dasar konstitusional dalam menghadapi ancaman siber dan perang hibrida. Namun, efektivitas tanggung jawab tersebut sangat ditentukan oleh sejauh mana regulasi nasional mampu beradaptasi terhadap karakter ancaman kontemporer. Dengan demikian, penelitian ini menekankan pada analisis kesenjangan antara norma konstitusional (UUD 1945) dengan implementasi regulasi positif dalam menghadapi ancaman multidimensi.

METODE

Penelitian ini menggunakan metode penelitian hukum normatif yuridis, yakni penelitian yang menempatkan hukum sebagai norma (*law in books*) yang berfungsi untuk mengkaji asas, doktrin, serta peraturan perundang-undangan yang berlaku (Soekanto & Mamudji, 2015). Fokus penelitian ini adalah menganalisis tanggung jawab negara menurut UUD 1945 dalam menghadapi ancaman siber dan perang hibrida, serta menilai sejauh mana kerangka hukum nasional yang ada memadai dalam merespons ancaman tersebut.

Pendekatan Penelitian

Penelitian hukum normatif ini menggunakan beberapa pendekatan, yaitu: Pendekatan Perundang-undangan (*statute approach*): dengan menelaah ketentuan konstitusional dalam UUD 1945 serta regulasi terkait, seperti UU No. 3 Tahun 2002 tentang Pertahanan Negara, UU No. 34 Tahun 2004 tentang TNI, dan UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Pendekatan Konseptual (*conceptual approach*): dengan mengkaji doktrin dan teori hukum yang relevan, seperti konsep state responsibility dalam hukum internasional dan teori pertahanan nasional. Pendekatan Komparatif (*comparative approach*): dengan membandingkan kebijakan pertahanan siber dan strategi menghadapi *hybrid warfare* di beberapa negara yang telah mengembangkan sistem hukum lebih adaptif

Sumber Bahan Hukum

Bahan hukum yang digunakan terdiri atas: Bahan hukum primer: Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, khususnya Pasal 30 tentang Sistem Pertahanan dan Keamanan Rakyat Semesta. Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, yang mengatur prinsip, sistem, dan penyelenggaraan pertahanan negara. Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, yang menegaskan peran TNI dalam menjaga kedaulatan dan keamanan nasional. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang mengatur tata kelola informasi elektronik, transaksi elektronik, serta larangan serangan siber. Undang-Undang Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara, yang menegaskan peran seluruh sumber daya nasional dalam pertahanan, termasuk dimensi non-militer. Peraturan pelaksana terkait keamanan siber, misalnya Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (BSSN). Bahan hukum sekunder: buku, artikel ilmiah, hasil penelitian terdahulu mengenai pertahanan negara, keamanan siber, dan perang hibrida (Asshiddiqie, 2020; Clarke & Knake, 2019; Pratama, 2022). Bahan hukum tersier: kamus hukum, ensiklopedia, dan sumber pendukung lain.

Teknik Pengumpulan dan Analisis

Bahan hukum dikumpulkan melalui studi kepustakaan (*library research*), baik dari peraturan perundang-undangan, jurnal, maupun literatur ilmiah lainnya. Analisis dilakukan

secara kualitatif deskriptif-analitis, yaitu menguraikan norma yang ada, kemudian mengevaluasi kecukupannya untuk menjawab permasalahan penelitian, serta menawarkan argumentasi hukum untuk perbaikan regulasi.

HASIL DAN PEMBAHASAN

Bentuk Tanggung Jawab Negara Menurut UUD 1945

Konstitusi memberikan mandat yang jelas mengenai tanggung jawab negara di bidang pertahanan dan keamanan. Pasal 30 ayat (2) UUD 1945 menyebutkan bahwa "usaha pertahanan dan keamanan negara dilaksanakan melalui sistem pertahanan dan keamanan rakyat semesta." Norma ini menempatkan negara sebagai aktor utama dengan TNI dan Polri sebagai kekuatan utama serta rakyat sebagai kekuatan pendukung.

Dalam menghadapi ancaman non-tradisional seperti serangan siber dan perang hibrida, bentuk tanggung jawab negara menurut UUD 1945 dapat dipahami dalam beberapa dimensi:

1. Tanggung jawab konstitusional → negara wajib menjamin kedaulatan dan keutuhan wilayah, baik dari serangan militer maupun ancaman non-militer. Artinya, meskipun Pasal 30 UUD 1945 tidak secara eksplisit menyebutkan "pertahanan siber", sifatnya yang terbuka memungkinkan penafsiran bahwa ancaman digital masuk dalam lingkup pertahanan negara
2. Tanggung jawab perlindungan warga negara → sejalan dengan Pasal 28G UUD 1945, negara berkewajiban melindungi setiap warga dari ancaman terhadap keselamatan pribadi, termasuk kebocoran data pribadi, serangan terhadap infrastruktur digital, serta disinformasi yang merusak tatanan demokrasi
3. Tanggung jawab pengaturan dan kebijakan → negara tidak cukup hanya menegaskan kewajiban secara normatif, tetapi harus menyusun regulasi, kebijakan, serta institusi yang efektif. Dalam hukum tata negara, tanggung jawab semacam ini dikenal sebagai *positive obligation* dari negara.

Dengan demikian, bentuk tanggung jawab negara menurut UUD 1945 dalam konteks ancaman siber dan perang hibrida adalah kewajiban menyeluruh: melindungi, mencegah, menanggulangi, serta memulihkan dampak serangan demi menjaga kedaulatan dan keamanan nasional.

Evaluasi Kerangka Hukum Nasional

Meskipun UUD 1945 memberikan mandat luas terkait tanggung jawab negara dalam bidang pertahanan dan keamanan, implementasi dalam regulasi positif di Indonesia masih menghadapi berbagai kelemahan. Analisis terhadap peraturan perundang-undangan menunjukkan beberapa celah hukum yang penting untuk diperhatikan:

a. UU No. 3 Tahun 2002 tentang Pertahanan Negara
   Undang-undang ini menegaskan bahwa pertahanan negara bersifat semesta, melibatkan seluruh warga negara, serta menekankan pada ancaman militer. Namun, dalam konteks ancaman siber dan perang hibrida, undang-undang ini belum memberikan payung hukum yang jelas. Tidak ada pasal yang secara eksplisit menyebutkan pertahanan siber sebagai bagian integral pertahanan nasional. Akibatnya, serangan siber yang berdampak

pada infrastruktur vital negara belum otomatis diposisikan sebagai ancaman terhadap kedaulatan, melainkan sering dipandang sebagai kejahatan teknologi semata.

b. UU No. 34 Tahun 2004 tentang TNI
   UU ini menegaskan tugas TNI untuk menjaga kedaulatan negara dari ancaman militer. Namun, ruang lingkup TNI dalam menghadapi ancaman non-militer, khususnya siber, tidak jelas. Akibatnya, terdapat tarik-menarik kewenangan antara TNI, Polri, dan BSSN. Dalam praktiknya, TNI kerap mengambil peran dalam *cyber defense*, tetapi dasar hukumnya tidak cukup kuat, sehingga menimbulkan ketidakpastian hukum (Santosa, 2020).
c. UU No. 2 Tahun 2002 tentang Kepolisian Negara RI
   UU ini memberikan mandat kepada Polri dalam menjaga keamanan dan ketertiban masyarakat, termasuk menangani *cybercrime*. Namun, ancaman siber yang dikategorikan sebagai kejahatan kriminal (misalnya penipuan online, pencurian data, atau hacking) berbeda dengan serangan siber bersifat strategis yang dapat melumpuhkan infrastruktur negara. Dengan kata lain, UU ini cenderung menempatkan ancaman siber sebagai masalah hukum pidana individual, bukan ancaman pertahanan nasional.
d. UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE)
   UU ITE lebih berfokus pada aspek pemanfaatan teknologi informasi, pengaturan transaksi elektronik, dan sanksi pidana terhadap penyalahgunaan teknologi. Namun, undang-undang ini tidak mengatur mekanisme pertahanan siber secara menyeluruh. Serangan yang berdampak pada keamanan nasional tetap diperlakukan sebatas pelanggaran pidana. Hal ini menunjukkan bahwa UU ITE hanya memenuhi aspek represif, bukan preventif dan strategis dalam kerangka pertahanan.
e. Perpres No. 53 Tahun 2017 jo. Perpres No. 133 Tahun 2022 tentang Badan Siber dan Sandi Negara (BSSN)
   Pembentukan BSSN merupakan langkah maju karena menghadirkan lembaga khusus di bidang siber. Akan tetapi, fungsi BSSN masih terbatas pada pengamanan sistem elektronik pemerintahan, perlindungan data, dan enkripsi. BSSN belum sepenuhnya terintegrasi dalam sistem pertahanan nasional, sehingga perannya lebih administratif dibanding strategis. Dalam konteks perang hibrida yang multidimensi, posisi BSSN ini masih lemah karena tidak memiliki mandat operasional untuk mengkoordinasikan pertahanan siber secara nasional.

Celah Hukum yang Teridentifikasi

1. Fragmentasi regulasi → peraturan tersebar dalam berbagai undang-undang dan peraturan presiden tanpa satu kerangka hukum terpadu, sehingga koordinasi antar-lembaga (TNI, Polri, BSSN, dan Kemenhan) sering kali tumpang tindih.
2. Tidak adanya strategi nasional eksplisit → Indonesia belum memiliki undang-undang atau kebijakan nasional yang secara komprehensif menyatukan upaya pertahanan siber dan menghadapi perang hibrida.
3. Orientasi regulasi masih represif → sebagian besar peraturan menekankan penegakan hukum setelah serangan terjadi (represif), bukan pada pencegahan (preventif) dan perlindungan (protektif).

Perbandingan Internasional

Sebagai perbandingan, Estonia telah mengintegrasikan strategi pertahanan siber ke dalam doktrin pertahanan nasional setelah mengalami *cyber attack* besar pada 2007. Strategi tersebut melibatkan koordinasi antara pemerintah, militer, sektor swasta, dan NATO dalam sistem deteksi dini dan mitigasi serangan.

Sementara itu, Singapura mengeluarkan *Cybersecurity Act 2018* yang menempatkan

siber sebagai bagian dari keamanan nasional. Undang-undang ini memberi kewenangan luas pada *Cyber Security Agency (CSA)* untuk mengawasi infrastruktur kritis dan menyusun kebijakan pertahanan siber nasional. Dari perbandingan tersebut, terlihat bahwa Indonesia masih tertinggal dalam menempatkan pertahanan siber sebagai bagian inti dari sistem pertahanan negara.

Implikasi terhadap Tanggung Jawab Negara

Kondisi hukum nasional sebagaimana diuraikan sebelumnya menunjukkan adanya kesenjangan mendasar antara mandat konstitusi dan realitas regulasi. UUD 1945 secara normatif memberikan mandat luas kepada negara untuk menjamin pertahanan dari segala bentuk ancaman, baik militer maupun non-militer. Namun, kerangka hukum positif Indonesia masih parsial, sektoral, dan lebih berorientasi pada ancaman konvensional. Hal ini menimbulkan beberapa implikasi serius terhadap pelaksanaan tanggung jawab negara:

1. Potensi Kegagalan Pemenuhan Kewajiban Konstitusional
   Apabila terjadi serangan siber berskala besar yang melumpuhkan infrastruktur vital—misalnya sistem perbankan nasional, jaringan listrik, atau pusat data pemerintahan—negara berpotensi gagal memenuhi kewajiban konstitusionalnya. Kegagalan ini bukan karena absennya norma konstitusi, melainkan lemahnya instrumen hukum turunan yang mampu mengoperasionalkan mandat konstitusional tersebut. Dalam perspektif hukum tata negara, kegagalan ini dapat dikategorikan sebagai bentuk constitutional failure, yakni ketika kewajiban normatif tidak terwujud dalam praktik karena ketiadaan instrumen pelaksana.
2. Dipertanyakannya Legitimasi Perlindungan Negara
   Negara juga memiliki tanggung jawab untuk melindungi warga negara sebagaimana diatur dalam Pasal 28G ayat (1) UUD 1945. Namun, ketika serangan siber menyebabkan kebocoran data pribadi jutaan warga atau disinformasi yang mengancam stabilitas politik, pertanyaan mengenai apakah negara telah menjalankan kewajiban perlindungan secara optimal menjadi relevan. Jika kerugian besar timbul akibat lemahnya sistem hukum dan kebijakan, maka legitimasi negara sebagai pelindung warganya dapat dipertanyakan. Hal ini berdampak langsung pada kepercayaan publik terhadap negara dan institusinya.
3. Orientasi Responsif dan Reaktif
   Hukum positif Indonesia saat ini lebih menekankan pendekatan represif, yakni menindak pelaku setelah serangan terjadi, bukan preventif atau protektif yang seharusnya menjadi ciri utama pertahanan negara. Akibatnya, Indonesia cenderung berada pada posisi reaktif, hanya merespons setelah ancaman nyata terjadi, alih-alih proaktif mencegah serangan sejak dini.. Kondisi ini berbeda dengan praktik di negara-negara yang lebih maju, di mana *cyber defense strategy* disusun untuk mengantisipasi, mendeteksi, dan merespons ancaman secara simultan.
4. Risiko Internasional dan Diplomasi Siber
   Implikasi lain yang sering diabaikan adalah dimensi internasional. Jika Indonesia tidak mampu melindungi infrastruktur sibernya, maka posisinya dalam diplomasi internasional akan lemah. Negara yang gagal membangun sistem pertahanan siber dapat dianggap tidak memenuhi standar *due diligence* dalam hukum internasional, sehingga berpotensi menimbulkan klaim tanggung jawab ketika serangan dari wilayah Indonesia merugikan negara lain. Dengan demikian, lemahnya regulasi nasional tidak hanya berdampak domestik, tetapi juga mengurangi kredibilitas Indonesia di tingkat global.

PENUTUP

Simpulan

Bentuk tanggung jawab negara menurut UUD 1945 dalam menghadapi ancaman siber dan perang hibrida meliputi kewajiban konstitusional untuk melindungi kedaulatan negara, keutuhan wilayah, serta keselamatan warga negara dari segala bentuk ancaman, baik militer maupun non-militer. Pasal 30 UUD 1945 menempatkan negara sebagai aktor utama dalam sistem pertahanan dan keamanan rakyat semesta (*Sishankamrata*), yang secara substantif dapat ditafsirkan mencakup ancaman kontemporer seperti siber dan hibrida.

Kerangka hukum nasional yang ada saat ini belum memadai dalam menjawab kompleksitas ancaman siber dan perang hibrida. UU Pertahanan, UU TNI, UU Polri, UU ITE, dan Perpres BSSN masih bersifat parsial, fragmentaris, dan lebih menekankan aspek represif. Akibatnya, koordinasi antar-lembaga belum terintegrasi dan strategi pertahanan siber nasional belum terbentuk secara komprehensif.

Kesenjangan antara norma konstitusional dan regulasi positif menimbulkan implikasi serius berupa potensi kegagalan negara memenuhi kewajiban konstitusional, lemahnya legitimasi perlindungan warga, orientasi hukum yang reaktif, serta menurunnya kredibilitas Indonesia dalam diplomasi siber internasional.

Keterbatasan

Penelitian ini memiliki keterbatasan pada ruang lingkup yang masih bersifat normatif dengan fokus pada analisis konstitusi dan regulasi nasional. Pendekatan empiris terkait implementasi kebijakan, efektivitas koordinasi antar-lembaga, maupun studi kasus serangan siber yang pernah terjadi di Indonesia belum dieksplorasi secara mendalam. Selain itu, perbandingan dengan strategi pertahanan siber negara lain masih terbatas pada telaah literatur, belum melalui kajian lapangan atau wawancara dengan pemangku kepentingan.

Saran

Legislasi: perlu dilakukan revisi terhadap UU No. 3 Tahun 2002 tentang Pertahanan Negara dengan menambahkan klausul khusus mengenai pertahanan siber dan perang hibrida sebagai bagian integral dari sistem pertahanan nasional.

Kelembagaan: pemerintah perlu memperkuat peran BSSN dengan kewenangan yang lebih luas dan terintegrasi, serta memperjelas koordinasi dengan TNI dan Polri dalam kerangka national *cyber defense strategy*.

Kebijakan strategis: diperlukan penyusunan doktrin pertahanan siber nasional yang proaktif, komprehensif, dan selaras dengan praktik terbaik internasional agar tanggung jawab negara sesuai UUD 1945 dapat terwujud secara optimal.

Penelitian lanjutan: disarankan adanya penelitian empiris mengenai efektivitas kebijakan dan kesiapan kelembagaan Indonesia dalam menghadapi serangan siber dan perang hibrida, termasuk perbandingan dengan negara-negara yang telah berhasil membangun sistem pertahanan siber nasional.

DAFTAR PUSTAKA

Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. Jurnal Keamanan Nasional, IX(2), 299–324.

Maharani, M. A., Atman, W., Ilmu, D., & Internasional, H. (2025). Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia Keamanan Siber sebagai Bagian dari Keamanan Nasional.

Pramono, B., & Pertahanan, U. (2025). Strategic adaptations for hybrid warfare : Enhancing Indonesian national defence in the digital. 8(6), 974–981. https://doi.org/10.53894/ijirss.v8i6.9776

Rafel. (2023). Referensi Hukum . In Referensi Hukum (Vol. 5, Issue 3, p. 15).

Supriyadi, A. A. (2025). INTEGRASI KEBIJAKAN PERTAHANAN DAN KEBIJAKAN PUBLIK DALAM PENANGGULANGAN ANCAMAN PERANG HIBRIDA : PENDEKATAN ANALISIS KEAMANAN NASIONAL INTEGRATION OF DEFENSE POLICY AND PUBLIC POLICY IN COUNTERING HYBRID WARFARE THREATS : A NATIONAL. 13(1), 1–17.

To, H. (2025). POTENSI ANCAMAN HIBRIDA PERANG SIBER DAN PERUBAHAN IKLIM TERHADAP INFRASTRUKTUR VITAL DAN KETAHANAN NASIONAL Aura Purify NATO STRATCOM (2021) menekankan pentingnya pendekatan integratif antara pertahanan siber dan adaptasi iklim dalam strategi keamanan nasional . Chertoff dan Simon (2022) (IPCC , WEF , NATO), serta dokumen kebijakan nasional dalam lima tahun terakhir .. Tahapan analisis meliputi : 1 . Identifikasi potensi ancaman dari kerentanan sektor infrastruktur melalui matriks. 12(2).

Wijanarko, T., Supriyadi, A. A., Saputro, G. E., Harefa, F., Kartiningsih, Y., & Mardamsyah, A. (2025). Model integrasi kebijakan pertahanan dan kebijakan publik mengatasi ancaman perang hibrida guna meningkatkan pertahanan negara. Online) |, 18(3), 2964–9056. www.plus62.isha.or.id/index.php/abdimas