DOI: https://doi.org/10.62017/syariah

TINJAUAN PENEGAKAN HUKUM DALAM INSTITUSI MILITER TERHADAP ANCAMAN *CYBER CRIME*

Farrah Nabillah *[1]
Irwan Triadi [2]

[1,2] Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta
*e-mail : 2310611024@mahasiswa.upnvj.ac.id, irwantriadi1@yahoo.com

Abstrak

Perkembangan teknologi digital telah mentransformasi operasi militer, termasuk di Indonesia, namun juga membawa ancaman serius berupa cyber crime yang dapat mengganggu keamanan nasional. Penelitian ini bertujuan menganalisis penegakan hukum cyber crime di lingkungan militer dengan pendekatan yuridis-normatif, mengkaji regulasi seperti UU ITE, UU TNI, dan KUHP Militer, serta membandingkannya dengan praktik di Amerika Serikat, China, dan Singapura. Rumusan masalah mencakup dua aspek: (1) Bagaimana Pengaturan Hukum Positif Cyber Crime di Lingkungan Militer?, dan (2) Bagaimana Implementasi Sanksi Hukum terhadap Cyber Crime?. Hasil penelitian menunjukkan bahwa meskipun UU ITE dan UU TNI menjadi dasar hukum utama, implementasinya di lingkungan militer masih menghadapi tantangan. Selain itu, disparitas antara KUHP Militer dan KUHP Nasional berpotensi menimbulkan inkonsistensi sanksi. Studi komparatif mengungkapkan bahwa negara-negara maju seperti Amerika Serikat, China, dan memiliki sistem pertahanan siber terintegrasi. Penelitian ini merekomendasikan perlunya harmonisasi regulasi, peningkatan kapasitas SDM siber militer, dan penguatan infrastruktur teknologi. Sinergi antara sanksi pidana dan disiplin militer juga dinilai krusial untuk memastikan penegakan hukum yang efektif sekaligus menjaga integritas institusi militer. Temuan ini memberikan kontribusi akademis dan praktis bagi pengembangan kebijakan pertahanan siber di Indonesia, khususnya dalam menghadapi ancaman digital yang semakin kompleks.

Kata Kunci: *Hukum Militer, Kejahatan Siber, Digital*

Abstract

The development of digital technology has transformed military operations, including in Indonesia, but it also brings serious threats in the form of cyber crime that can disrupt national security. This research aims to analyze the law enforcement of cyber crime in the military environment with a juridical-normative approach, examining regulations such as the ITE Law, TNI Law, and Military Criminal Code, and comparing them with practices in the United States, China, and Singapore. The formulation of the problem includes two aspects: (1) How is the positive legal regulation of cyber crime in the military environment?, and (2) How is the implementation of legal sanctions against cyber crime?. The results show that although the ITE Law and TNI Law are the main legal basis, their implementation in the military environment still faces challenges. In addition, the disparity between the Military Criminal Code and the National Criminal Code has the potential to cause inconsistencies in sanctions. Comparative studies reveal that developed countries such as the United States, China, and have integrated cyber defense systems. This study recommends the need for regulatory harmonization, increasing the capacity of military cyber human resources, and strengthening technological infrastructure. The synergy between criminal sanctions and military discipline is also considered crucial to ensure effective law enforcement while maintaining the integrity of military institutions. These findings provide academic and practical contributions to the development of cyber defense policies in Indonesia, especially in the face of increasingly complex digital threats.

Keywords: *military law, cybercrime, digital*

PENDAHULUAN

Perkembangan teknologi digital yang begitu pesat telah membawa transformasi besar-besaran di berbagai aspek kehidupan, tak terkecuali di dunia militer yang kini semakin mengandalkan kecanggihan teknologi informasi dan komunikasi (TIK) sebagai tulang punggung operasionalnya. Di masa lalu, strategi militer sangat bergantung pada kekuatan fisik, jumlah pasukan, dan logistik konvensional, namun kini semua itu telah berubah dengan hadirnya berbagai inovasi teknologi mutakhir. Tentara Nasional Indonesia (TNI) sebagai contoh, telah mengadopsi sistem komunikasi satelit yang memungkinkan koordinasi real-time di medan

DOI: https://doi.org/10.62017/syariah

operasi, menggunakan drone pengintai untuk pengawasan strategis, serta memanfaatkan analisis big data untuk memprediksi pergerakan musuh dan menyusun taktik berbasis data. Revolusi digital ini tidak sekadar mempermudah pertukaran informasi antar kesatuan, tetapi benar-benar mentransformasi paradigma operasi militer menjadi lebih efisien, akurat, dan komprehensif memungkinkan TNI untuk melakukan pengawasan wilayah yang lebih luas, mengidentifikasi ancaman dengan presisi tinggi, serta mengambil keputusan operasional dalam waktu singkat yang sangat krusial di medan pertempuran modern.

Di balik segala kemudahan yang ditawarkan oleh pesatnya perkembangan teknologi digital, tersembunyi pula ancaman baru yang jauh lebih rumit dan multidimensi, terutama dalam bentuk kejahatan siber yang mampu menggerogoti sendi-sendi keamanan dan kedaulatan suatu negara.[1] Dunia militer yang kini begitu bergantung pada infrastruktur digital menjadi sangat rentan terhadap berbagai bentuk serangan siber canggih mulai dari sabotase sistem komando yang bisa melumpuhkan koordinasi pasukan, pembobolan data intelijen strategis yang berisi informasi sensitif, hingga gangguan komunikasi yang dapat memecah konsentrasi operasi militer di saat-saat kritis. Menyadari kerentanan ini, TNI tidak tinggal diam, mereka secara proaktif membangun benteng pertahanan siber melalui pembentukan Satuan Siber khusus yang dilengkapi dengan teknologi mutakhir dan personel terlatih. Upaya ini diperkuat dengan program pelatihan intensif untuk meningkatkan literasi digital prajurit, pengembangan sistem deteksi dini serangan siber, serta kerja sama dengan berbagai pihak untuk menciptakan ekosistem keamanan siber yang tangguh. Langkah-langkah strategis ini tidak hanya bertujuan untuk memproteksi aset digital militer, tetapi juga menjadi tameng nasional dalam menghadapi dinamika perang modern yang semakin tidak terlihat namun dampaknya bisa sangat nyata, bahkan berpotensi mengancam stabilitas negara jika tidak diantisipasi dengan serius.

Di tengah pesatnya transformasi digital di lingkungan militer, muncul kebutuhan mendesak untuk membangun kerangka hukum yang komprehensif dan adaptif guna mengatur penggunaan teknologi siber dalam operasi militer sebuah tantangan yang tidak bisa dianggap remeh.[2] Hukum militer saat ini dituntut untuk terus berevolusi, tidak hanya sekadar mengikuti perkembangan teknologi yang bergerak cepat, tetapi juga harus mampu menjembatani kepentingan operasional dengan kepatuhan terhadap berbagai regulasi nasional seperti UU Siber dan UU Pertahanan Negara, serta kesepakatan internasional seperti Konvensi Budapest tentang kejahatan siber. Transformasi digital di tubuh TNI sesungguhnya bukan semata-mata persoalan membeli peralatan canggih atau mengadopsi sistem terbaru, melainkan sebuah revolusi menyeluruh yang mencakup tiga pilar utama, penguatan infrastruktur teknologi, peningkatan kapasitas prajurit melalui pendidikan literasi digital berkelanjutan, dan yang tak kalah penting penyempurnaan aspek legal yang menjadi payung hukum semua aktivitas siber militer. Prajurit masa kini tidak hanya harus terampil mengoperasikan drone atau sistem *cyber warfare*, tetapi juga perlu memahami batasan hukum dalam melakukan operasi siber ofensif maupun defensif.[3] Sinergi ketiga elemen inilah yang akan menjadi pondasi kokoh bagi pertahanan siber Indonesia, memastikan setiap langkah digital TNI tetap berada dalam koridor hukum yang jelas, sekaligus memberikan perlindungan maksimal terhadap kedaulatan negara di dunia maya yang penuh dengan ketidakpastian dan ancaman tak kasat mata. Tanpa keseimbangan ini, kemajuan teknologi justru bisa menjadi bumerang yang mengancam stabilitas nasional di era di mana perang siber bisa lebih berbahaya daripada konvensional.

Dinamika hukum militer dalam menghadapi tantangan kejahatan siber di era digital menuntut analisis mendalam tentang pengaturan hukum positif terkait penegakan hukum *cyber*

[1] Chiara Belva Chatlina, Aji Mulyana, and Mia Amalia, "Pengaruh Perkembangan Teknologi Informasi Dan Komunikasi Terhadap Kualitas Hubungan Sosial Dalam Keluarga," *KOMUNITAS: Jurnal Ilmu Sosiologi* 7, no. 1 (2024): 19–38.
[2] Farly Mochamad, "Menjaga Kedaulatan Di Era Digital: Peran TNI Dalam Pertahanan Siber Di Indonesia," *Kompasiana*, September 5, 2024,
[3] Rifla Mufarihana Zahira, "Dinamika Hukum Telematikan Dalam Era Digital: Perlindungan Privasi Dan Keamanan Data Di Indonesia" 2, no. 2 (2025): 211–20.

DOI: https://doi.org/10.62017/syariah

crime di lingkungan militer serta penegakan hukum sesuai hukum positif dan perbandingan dengan praktik negara lain.[4] Namun, di balik upaya penegakan hukum yang dilakukan, masih ada kelemahan regulasi yang harus ditelaah lebih mendalam. Misalnya, ketidakjelasan aturan mengenai beberapa jenis kejahatan siber, minimnya detail regulasi yang dapat menyesuaikan diri dengan perkembangan modus operandi kejahatan dunia maya, serta kendala infrastruktur dan SDM yang kurang mumpuni dalam menangani kasus-kasus di lingkungan militer. Kelemahan-kelemahan ini dapat dieksploitasi oleh pelaku kriminal dan menjadi hambatan besar bagi upaya penegakan hukum di lembaga militer.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis-normatif dengan mengkaji berbagai peraturan perundang-undangan terkait hukum militer dan kejahatan siber, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta pengaturan hukum negara lain. Analisis dilakukan terhadap aspek normatif hukum yang berlaku, termasuk celah regulasi dan ketidaksesuaian antara perkembangan teknologi siber dengan kerangka hukum yang ada.

Selain itu, penelitian ini juga mengkaji putusan pengadilan, doktrin hukum, dan literatur akademis untuk mengevaluasi efektivitas penegakan hukum militer dalam menghadapi kejahatan siber. Dengan pendekatan ini, penelitian bertujuan memberikan rekomendasi untuk penyempurnaan regulasi dan kebijakan yang lebih adaptif terhadap tantangan digital di lingkungan militer.

PEMBAHASAN

1. Pengaturan Hukum Positif Cyber Crime di Lingkungan Militer

Analisis terhadap peran Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam lingkup militer mengungkapkan bahwa regulasi ini berfungsi sebagai dasar hukum utama dalam menangani kejahatan siber, termasuk yang terjadi di lingkungan militer.[5] UU ITE mencakup berbagai bentuk tindak pidana digital yang dapat membahayakan keamanan dan pertahanan negara, misalnya peretasan sistem elektronik atau penyebaran konten yang berpotensi mengganggu stabilitas operasi militer. Namun, penerapan UU ITE di institusi militer membutuhkan adaptasi lebih lanjut agar selaras dengan karakteristik unik militer, seperti hierarki kaku, kerahasiaan operasi, dan kebutuhan disiplin yang tinggi. Tanpa penyesuaian tersebut, terdapat risiko ketidakjelasan hukum yang dapat memengaruhi kepastian hukum bagi prajurit sebagai subjek hukum sekaligus pelaku tugas pertahanan.[6] Selain itu, dinamika kejahatan siber yang terus berkembang menuntut pembaruan regulasi secara berkala agar tetap relevan dalam menghadapi ancaman digital yang semakin canggih.

Di sisi lain, kewenangan militer dalam menangani *cyber crime* diatur secara khusus dalam Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI) beserta peraturan turunannya.[7] Regulasi ini memberikan mandat kepada TNI untuk melindungi kedaulatan negara, termasuk melalui pertahanan siber yang terkoordinasi dengan instansi terkait. Dalam menjalankan tugasnya, TNI memiliki otoritas untuk melakukan langkah-langkah

[4] Fadhila Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum* 2, no. 1 (2024): 8–16, https://doi.org/10.32520/albahts.v2i1.3044.

[5] Republik Indonesia, "Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Sekretariat Negara*, 2024.

[6] Humas, "Implementasi Undang-Undang ITE Harus Berikan Rasa Keadilan Di Tengah Masyarakat," *Sekretariat Kabinet Republik Indonesia*, February 15, 2021, https://setkab.go.id/implementasi-undang-undang-ite-harus-berikan-rasa-keadilan-di-tengah-masyarakat/.

[7] Republik Indonesia, "Undang-Undang (UU) Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia," *Sekretariat Negara*, 2004.

DOI: https://doi.org/10.62017/syariah

pencegahan, investigasi, dan pemulihan terhadap serangan siber yang mengancam aset militer atau infrastruktur strategis nasional. Namun, pelaksanaan kewenangan ini harus tetap berpegang pada prinsip-prinsip hukum yang berlaku, seperti proporsionalitas, akuntabilitas, dan penghormatan terhadap hak asasi manusia. Tantangan utamanya adalah menyeimbangkan antara kebutuhan operasional militer yang seringkali bersifat rahasia dengan tuntutan transparansi dan kepatuhan hukum. Oleh karena itu, diperlukan mekanisme pengawasan yang jelas agar upaya penegakan hukum siber di lingkungan militer tidak justru menimbulkan pelanggaran atau penyalahgunaan wewenang.

Aspek terakhir yang krusial dalam penanganan kejahatan siber di lingkungan militer adalah perlunya penyelarasan antara Kitab Undang-Undang Hukum Pidana (KUHP) Militer dengan KUHP Nasional. KUHP Militer secara khusus mengatur berbagai bentuk pelanggaran yang dilakukan oleh personel militer dalam konteks pelaksanaan tugas dan pelanggaran disiplin militer, sementara KUHP Nasional berlaku untuk tindak pidana umum di masyarakat. Dalam implementasinya, seringkali muncul kerumitan yuridis ketika suatu tindak pidana siber yang dilakukan anggota militer memiliki unsur baik pelanggaran disiplin militer maupun tindak pidana umum. Ketidakselarasan antara kedua regulasi ini berpotensi menimbulkan dualisme penanganan kasus, tumpang tindih kewenangan lembaga peradilan militer dan umum, serta inkonsistensi dalam penerapan sanksi.[8] Oleh karena itu, harmonisasi menyeluruh antara kedua instrumen hukum ini mutlak diperlukan untuk menciptakan kepastian hukum, menghindari konflik kewenangan, sekaligus memastikan penegakan hukum yang efektif dan proporsional. Selain itu, sinkronisasi ini juga harus mempertimbangkan keseimbangan antara prinsip keadilan bagi personel militer sebagai warga negara dengan kebutuhan khusus institusi militer dalam menjaga disiplin dan keamanan internal, yang pada akhirnya akan berkontribusi pada perlindungan yang lebih komprehensif terhadap keamanan dan pertahanan nasional.

2. Implementasi Sanksi Hukum terhadap *Cyber Crime*

Berbagai kasus pelanggaran kejahatan siber yang terjadi di lingkungan Tentara Nasional Indonesia (TNI) membuktikan adanya ancaman serius terhadap infrastruktur digital institusi pertahanan nasional. Walaupun belum banyak kasus yang terungkap secara publik melibatkan personel militer secara langsung, beberapa insiden besar seperti kebocoran data sensitif di instansi pemerintah dan serangan siber terhadap lembaga strategis seperti Kepolisian Republik Indonesia (Polri) serta berbagai kementerian menunjukkan kerentanan sistem yang berpotensi pula terjadi di tubuh TNI.[9] Ancaman ini mencakup berbagai bentuk, mulai dari infiltrasi sistem komputer, gangguan operasional berbasis digital, hingga pencurian informasi rahasia yang dapat membahayakan kedaulatan negara. Menyikapi hal ini, TNI telah mengambil langkah proaktif dengan membentuk unit patroli siber dan menjalin kerja sama strategis dengan Polri, menunjukkan komitmen tinggi dalam membangun pertahanan siber yang tangguh.

Meskipun upaya penanggulangan telah dilakukan, pelaksanaan penegakan hukum terhadap kejahatan siber di lingkungan militer masih dihadapkan pada berbagai tantangan multidimensional. Dari aspek hukum, belum adanya kejelasan mengenai pembagian kewenangan antara otoritas militer dan sipil dalam menangani kasus siber sering menimbulkan dualisme penanganan dan ketidakpastian hukum.[10] Pada tataran operasional, minimnya jumlah ahli siber militer yang kompeten serta keterbatasan fasilitas teknologi mutakhir menjadi penghambat utama dalam melaksanakan fungsi pengamanan secara efektif. Tantangan ini semakin kompleks

[8] Agus Sahbani, "Pasal UU ITE Diserap Dalam RKUHP Hingga 5 Agenda Prioritas Panglima TNI Baru," *Hukumonline.Com*, December 1, 2022, https://www.hukumonline.com/berita/a/pasal-uu-ite-diserap-dalam-rkuhp-hingga-5-agenda-prioritas-panglima-tni-baru-lt638743a481da3/.

[9] Mujtahidin, "Patroli Siber TNI Kolaborasi Cyber Crime Polri, Endus Informasi Hoax Di Medsos," *Rri.Co.Id*, September 10, 2024, https://rri.co.id/pilkada-2024/964990/patroli-siber-tni-kolaborasi-cyber-crime-polri-endus-informasi-hoax-di-medsos.

[10] Riza Aslam Khaeran, "Pro Dan Kontra Keterlibatan Militer Dalam Keamanan Siber," *Metro TV News*, 2025, https://www.metrotvnews.com/read/KZmCVxXZ-pro-dan-kontra-keterlibatan-militer-dalam-keamanan-siber.

DOI: https://doi.org/10.62017/syariah

mengingat modus operandi pelaku kejahatan siber yang terus berevolusi dengan teknik yang semakin canggih dan jaringan yang terstruktur rapi. Kondisi ini memerlukan penyelesaian komprehensif yang meliputi penyempurnaan regulasi, peningkatan kapasitas SDM, serta penguatan infrastruktur teknologi pertahanan siber.

Dalam perspektif komparatif dengan negara-negara maju seperti Amerika Serikat, China, dan Singapura, pendekatan penanganan kejahatan siber di lingkungan militer Indonesia menunjukkan perbedaan yang cukup mencolok dalam hal struktur, strategi, dan kapabilitas. Amerika Serikat melalui U.S. *Cyber Command*-nya telah membangun sistem pertahanan siber yang sangat maju dan terintegrasi penuh dengan arsitektur pertahanan nasional, dilengkapi dengan mandat operasional yang luas mencakup baik fungsi defensif maupun ofensif. [11] China mengembangkan model yang unik dengan menyinergikan secara ketat kemampuan militer dan sipil melalui pendekatan terpusat di bawah kendali pemerintah pusat, didukung oleh regulasi yang sangat ketat dan sistem pengawasan ekstensif.[12] Sementara itu, Singapura sebagai negara kecil namun maju secara teknologi menerapkan paradigma kolaboratif yang melibatkan kemitraan strategis antara militer dengan berbagai lembaga sipil, disertai investasi besar-besaran dalam pengembangan SDM berkualitas tinggi dan infrastruktur teknologi mutakhir. [13] Perbandingan ini mengungkapkan bahwa Indonesia masih perlu melakukan berbagai langkah strategis, termasuk memperkuat mekanisme koordinasi antar lembaga pertahanan dan keamanan, meningkatkan kapasitas teknis melalui pengembangan SDM spesialis siber, serta menyempurnakan kerangka regulasi untuk menciptakan sistem penegakan hukum yang lebih komprehensif dan adaptif terhadap dinamika ancaman siber kontemporer di lingkungan militer.

Analisis mendalam terhadap penerapan sanksi pidana dan disiplin militer dalam menangani pelaku kejahatan siber di lingkungan militer mengungkapkan bahwa kedua mekanisme ini memiliki peran yang saling melengkapi namun dengan tujuan yang berbeda secara fundamental. Sanksi pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) berfungsi sebagai instrumen hukum yang bersifat umum, bertujuan untuk menciptakan efek jera, memulihkan keadilan, serta melindungi kepentingan masyarakat luas. Di sisi lain, sanksi disiplin militer yang diatur dalam peraturan internal militer lebih berfokus pada pemeliharaan tata tertib, hierarki, dan nilai-nilai korps yang menjadi pilar utama organisasi kemiliteran. Dalam konteks operasional, penanganan kasus kejahatan siber di lingkungan militer membutuhkan pendekatan holistik yang mengintegrasikan kedua sistem sanksi ini secara sinergis, di mana pelaku tidak hanya harus mempertanggungjawabkan perbuatannya di depan pengadilan umum atau militer, tetapi juga wajib menjalani proses pembinaan khusus melalui mekanisme disiplin militer untuk memastikan adanya perubahan perilaku dan pemahaman mendalam tentang etika profesi militer. Pendekatan terpadu semacam ini sangat krusial untuk mempertahankan profesionalisme, soliditas, dan kepercayaan publik terhadap institusi militer di era digital, sekaligus memastikan bahwa penanganan setiap kasus kejahatan siber tidak hanya menyelesaikan aspek hukumnya saja, tetapi juga memperkuat ketahanan internal organisasi militer terhadap berbagai bentuk ancaman siber yang semakin kompleks di masa depan.

KESIMPULAN

Penegakan hukum terhadap *cyber crime* di lingkungan militer Indonesia memerlukan pendekatan multidimensi yang mencakup aspek regulasi, operasional, dan sumber daya manusia. Meskipun UU ITE dan UU TNI telah menjadi landasan hukum utama, tantangan seperti

[11] Bielqis Sahara et al., "Perbandingan Hukum Pidana Terhadap Kejahatan Dunia Maya Di Indonesia Dan Amerika Serikat" 07, no. 2 (2025): 97–112.
[12] Nadia Talita Putri et al., "Penanganan Cyber Attacks Oleh Pemerintah Tiongkok Melalui Kebijakan Network Security Tahun 2000-2015," *Jurnal Dikshi: Diskusi Ilmiah Komunitas Hubungan Internasional* 1, no. 1 (2017): 1–12.
[13] Syadid Jiddan Alharun, "Perbandingan Hukum Tindak Pidana Siber Antara Indonesia Dengan Singapura" 11, no. 1 (2025): 1–23.

ketidakjelasan kewenangan antara lembaga militer dan sipil, disparitas antara KUHP Militer dan KUHP Nasional, serta keterbatasan infrastruktur dan SDM masih menjadi hambatan signifikan. Perbandingan dengan negara-negara seperti Amerika Serikat, China, dan Singapura menunjukkan pentingnya integrasi sistem pertahanan siber, harmonisasi regulasi, dan investasi dalam pengembangan kapasitas teknis. Untuk itu, diperlukan penyempurnaan kerangka hukum yang adaptif, peningkatan kolaborasi antarlembaga, dan penguatan sinergi antara sanksi pidana dengan disiplin militer guna menciptakan mekanisme penegakan hukum yang efektif dan berkeadilan. Dengan implementasi kebijakan yang holistik, TNI tidak hanya dapat mengatasi ancaman siber yang semakin kompleks tetapi juga memastikan keberlanjutan pertahanan nasional di era digital, sekaligus menjaga integritas dan profesionalisme sebagai institusi yang menjadi tulang punggung kedaulatan negara. Temuan ini diharapkan dapat menjadi acuan bagi pengembangan kebijakan pertahanan siber Indonesia ke depan, baik dalam konteks akademis maupun praktis.

REFERENSI

Jurnal

Alharun, Syadid Jiddan. "Perbandingan Hukum Tindak Pidana Siber Antara Indonesia Dengan Singapura" 11, no. 1 (2025): 1–23.

Chatlina, Chiara Belva, Aji Mulyana, and Mia Amalia. "Pengaruh Perkembangan Teknologi Informasi Dan Komunikasi Terhadap Kualitas Hubungan Sosial Dalam Keluarga." *KOMUNITAS: Jurnal Ilmu Sosiologi* 7, no. 1 (2024): 19–38.

Humas. "Implementasi Undang-Undang ITE Harus Berikan Rasa Keadilan Di Tengah Masyarakat." *Sekretariat Kabinet Republik Indonesia*, February 15, 2021. https://setkab.go.id/implementasi-undang-undang-ite-harus-berikan-rasa-keadilan-di-tengah-masyarakat/.

Khaeran, Riza Aslam. "Pro Dan Kontra Keterlibatan Militer Dalam Keamanan Siber." *Metro TV News*, 2025. https://www.metrotvnews.com/read/KZmCVxXZ-pro-dan-kontra-keterlibatan-militer-dalam-keamanan-siber.

Mochamad, Farly. "Menjaga Kedaulatan Di Era Digital: Peran TNI Dalam Pertahanan Siber Di Indonesia." *Kompasiana*, September 5, 2024. https://www.kompasiana.com/farlymochamad2616/66d95848c925c47055561592/menjaga-kedaulatan-di-era-digital-peran-tni-dalam-pertahanan-siber-di-indonesia.

Mujtahidin. "Patroli Siber TNI Kolaborasi Cyber Crime Polri, Endus Informasi Hoax Di Medsos." *Rri.Co.Id*, September 10, 2024. https://rri.co.id/pilkada-2024/964990/patroli-siber-tni-kolaborasi-cyber-crime-polri-endus-informasi-hoax-di-medsos.

Putri, Nadia Talita, Idin Fasisaka, A A B Surya, and Widya Nugraha. "Penanganan Cyber Attacks Oleh Pemerintah Tiongkok Melalui Kebijakan Network Security Tahun 2000-2015." *Jurnal Dikshi: Diskusi Ilmiah Komunitas Hubungan Internasional* 1, no. 1 (2017): 1–12.

Rahman Najwa, Fadhila. "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber Di Indonesia." *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum* 2, no. 1 (2024): 8–16. https://doi.org/10.32520/albahts.v2i1.3044.

Sahara, Bielqis, Salsabilah Maharani, Nurul Khatama Putri, Suci Rusmiarni, Septi Emiliyah, Nesta Putra Side, Asep Suherman, and Universitas Bengkulu. "Perbandingan Hukum Pidana Terhadap Kejahatan Dunia Maya Di Indonesia Dan Amerika Serikat" 07, no. 2 (2025): 97–112.

Sahbani, Agus. "Pasal UU ITE Diserap Dalam RKUHP Hingga 5 Agenda Prioritas Panglima TNI Baru." *Hukumonline.Com*, December 1, 2022. https://www.hukumonline.com/berita/a/pasal-uu-ite-diserap-dalam-rkuhp-hingga-5-agenda-prioritas-panglima-tni-baru-lt638743a481da3/.

Zahira, Rifla Mufarihana. "Dinamika Hukum Telematikan Dalam Era Digital: Perlindungan Privasi Dan Keamanan Data Di Indonesia" 2, no. 2 (2025): 211–20.

DOI: https://doi.org/10.62017/syariah

Peraturan Perundang-Undangan

Undang-Undang Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia.

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.