Jurnal RechtsVinding Media Pembinaan Hukum Nasional
ISSN 2089-9009
Volume 14 Nomor 2, Agustus 2025

POTENSI KONFLIK KEWENANGAN PADA PERLINDUNGAN DARI ANCAMAN SIBER DI INDONESIA

Potential Conflicts of Authority in Cyber Threat Protection in Indonesia

Ahmad Rizal Roby Ananta
Fakultas Hukum, Universitas Airlangga
Gedung A.G. Pringgodigdo, Jl. Dharmawangsa Dalam Selatan, Airlangga,
Kec. Gubeng, Surabaya, Jawa Timur 60286
e-mail: ahmad.rizal.roby-2024@fh.unair.ac.id

Indrawati
Fakultas Hukum, Universitas Airlangga
Gedung A.G. Pringgodigdo, Jl. Dharmawangsa Dalam Selatan, Airlangga,
Kec. Gubeng, Surabaya, Jawa Timur 60286
e-mail: indrawati@fh.unair.ac.id

Demas Brian Wicaksono
Fakultas Hukum, Universitas 17 Agustus 1945 Banyuwangi
Jl. Adi Sucipto No.26, Taman Baru,
Kec. Banyuwangi, Kabupaten Banyuwangi, Jawa Timur 68418
e-mail: demasbrian@untag-banyuwangi.ac.id

Istikhomah
Fakultas Hukum, Universitas Airlangga
Gedung A.G. Pringgodigdo, Jl. Dharmawangsa Dalam Selatan, Airlangga,
Kec. Gubeng, Surabaya, Jawa Timur 60286
e-mail: istikhomah-2024@fh.unair.ac.id

Zaskiya Amalina
Fakultas Hukum, Universitas Airlangga
Gedung A.G. Pringgodigdo, Jl. Dharmawangsa Dalam Selatan, Airlangga,
Kec. Gubeng, Surabaya, Jawa Timur 60286
e-mail: zaskiya.amalina-2024@fh.unair.ac.id

Abstrak

Permasalahan keamanan siber kini menjadi isu strategis bagi Indonesia, menyusul berbagai serangan digital seperti peretasan Pusat Data Nasional dan gangguan pada aplikasi SatuSehat. Fenomena ini mengindikasikan lemahnya ketahanan digital nasional serta tidak terpadunya koordinasi antar instansi. Penelitian ini mengkaji potensi konflik kewenangan antara Badan Siber dan Sandi Negara (BSSN), Tentara Nasional Indonesia (TNI), dan Kepolisian Republik Indonesia (Polri) dalam konteks perlindungan terhadap ancaman siber. Pendekatan yang digunakan dalam penelitian ini adalah yuridis normatif dengan mengadopsi pendekatan konseptual, pendekatan peraturan perundang-undangan, serta pendekatan kasus. Temuan menunjukkan bahwa belum adanya kejelasan batas tugas dan tanggung jawab masing-masing lembaga menjadi akar dari tumpang tindih kewenangan. Oleh karena itu, dibutuhkan penyusunan regulasi turunan berbasis ius constituendum yang menegaskan pembagian peran, pola koordinasi, serta prosedur operasional antar lembaga. Kesimpulan dari penelitian ini menegaskan pentingnya sinergi struktural yang berbasis hukum agar Indonesia memiliki sistem keamanan siber yang responsif dan terintegrasi. Rekomendasi ditujukan kepada pemerintah untuk segera membentuk regulasi teknis sebagai solusi konkret terhadap permasalahan tersebut.

Kata Kunci: Ketahanan Siber, Kejahatan Siber, Lembaga Negara.

Abstract

Cybersecurity has emerged as a strategic issue for Indonesia following a series of digital attacks, such as the hacking of the National Data Center and the SatuSehat application. These incidents reflect the vulnerability of the nation's digital infrastructure and highlight the lack of effective coordination among state institutions. This study explores the potential authority conflicts among the National Cyber and Crypto Agency (BSSN), the Indonesian National Armed Forces (TNI), and the Indonesian National Police (Polri) in addressing cyber threats. The research applies a normative legal method with conceptual, statutory, and case-based approaches. The findings indicate that the absence of clear legal frameworks defining institutional roles and responsibilities contributes to overlapping mandates. Therefore, it is essential to formulate implementing regulations based on the ius constituendum to ensure precise authority delineation, operational procedures, and coordination mechanisms among the three institutions. The study concludes that legal reform and structural synergy are vital for developing an integrated and responsive national cybersecurity system. The recommendation calls for the government to establish a detailed regulatory framework to resolve potential inter-agency authority conflicts in Indonesia's cyber defense.

Keywords: *Cyber Resilience, Cybercrime, State Institutions.*

A. Pendahuluan

Negara didasarkan pada peraturan perundang-undangan yang sah sebagai dasar legitimasi dalam pelaksanaan tugasnya[1]. Kewenangan tersebut menjadi bagian tak terpisahkan dari fungsi institusi yang dibentuk dalam kerangka negara hukum. Tujuan utama dari pemberian hak ini adalah menjamin keberlangsungan pemerintahan yang efektif dan bertanggung jawab[2]. Namun demikian, pelaksanaan kewenangan antar lembaga tidak jarang menimbulkan konflik kepentingan apabila terjadi tumpang tindih dalam praktiknya. Kondisi ini memperlihatkan kompleksitas relasi kelembagaan yang perlu diselesaikan secara hukum dan administratif.

Bidang keamanan siber merupakan salah satu contoh di mana tumpang tindih kewenangan mulai terlihat, khususnya dalam penanganan ancaman digital seperti perangkat lunak berbahaya[3]. Awalnya, fungsi ini dijalankan oleh Badan Siber dan Sandi Negara (BSSN) sebagai satu-satunya otoritas. Akan tetapi, dengan meningkatnya ancaman digital dan kebutuhan koordinasi lintas sektor, dua lembaga lain Polri dan TNI mulai ikut mengambil peran[4]. Pelibatan keduanya bertujuan untuk memperluas jangkauan perlindungan, tetapi juga menghadirkan tantangan koordinasi dan pembagian peran. Hal ini secara langsung menimbulkan potensi konflik kewenangan di antara ketiga institusi tersebut.

Meskipun Polri dan TNI memiliki garis fungsi yang jelas dalam sistem keamanan Polri untuk keamanan dalam negeri dan TNI untuk pertahanan eksternal dalam konteks ancaman siber, batas-batas tersebut menjadi kabur. Ancaman siber sering kali tidak mengenal batas yurisdiksi, sehingga menuntut pendekatan yang terpadu dan lintas sektoral[5]. Ketidaktegasan dalam pembagian peran dapat menimbulkan kebingungan dalam pelaksanaan kebijakan di lapangan. Ini bukan hanya menghambat respons terhadap ancaman[6], tetapi juga membuka kemungkinan sengketa kewenangan. Jika tidak segera ditangani, hal ini akan melemahkan sistem keamanan siber nasional.

Masalah yang lebih spesifik muncul ketika tidak terdapat aturan teknis yang mengatur pola kerja sama dan struktur koordinasi antar lembaga yang terlibat[7]. Tanpa mekanisme

---

1 I Nengah Sudiarta, "Pengaturan Hak Asasi Manusia Dalam Sistem Hukum Nasional," *IJOLARES : Indonesian Journal of Law Research* 2, no. 1 (30 Maret 2024): 25, https://doi.org/10.60153/ijolares.v2i1.44.

2 Anugrah Anugrah dan Rahmat Rahmat, "Pendidikan Karakter dalam Perspektif Kurikulum Pendidikan Pancasila dan Kewarganegaraan (PPKn)," *Jurnal Pendidikan dan Pembelajaran Indonesia (JPPI)* 4, no. 1 (9 Juni 2024): 26, https://doi.org/10.53299/jppi.v4i1.403.

3 Eko Haryadi Haryadi dkk., "Identifikasi Ancaman Keamanan Siber Dari Penyalahgunaan Sumber Daya Tik: Studi Kasus Perusahaan Polymer," *Technologia : Jurnal Ilmiah* 15, no. 4 (8 Oktober 2024): 887, https://doi.org/10.31602/tji.v15i4.16429.

4 Wahyu Wachid Anshory, "Peran Baru TNI Perangi Ancaman Siber, Apa Bedanya dengan Komdigi dan BSSN?," *kompas.com*, 26 Maret 2025, https://www.kompas.com/jawa-barat/read/2025/03/26/173000488/peran-baru-tni-perangi-ancaman-siber-apa-bedanya-dengan-komdigi-dan.

5 Agus Haryanto dan Satya Muhammad Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal* 7, no. 1 (30 April 2023): 56–69, https://doi.org/10.34010/gpsjournal.v7i1.8141.

6 Agus Haryanto dan Satya Muhammad Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal* 7, no. 1 (30 April 2023): 60, https://doi.org/10.34010/gpsjournal.v7i1.8141.

7 Yunni Widhi Astuti, "Peran Masyarakat Dalam Pembentukan Aturan Hukum The Role of Society in Forming the Rule of Law," *Ethics and Law Journal: Business and Notary* 1, no. 3 (28 Desember 2023): 267, https://doi.org/10.61292/ELJBN.77.

yang jelas, respons terhadap serangan siber bisa menjadi lambat dan tidak terkoordinasi. Perbedaan sistem internal dan budaya kelembagaan antar institusi juga menambah kompleksitas pelaksanaan operasional. Dalam situasi kritis, hal ini dapat menjadi celah yang mengancam kestabilan keamanan nasional secara keseluruhan. Oleh karena itu, kebutuhan akan regulasi yang detail dan implementatif menjadi sangat mendesak[8].

Selain berdampak pada aspek operasional, sengketa kewenangan juga dapat menurunkan kepercayaan publik terhadap kapasitas negara dalam menjaga keamanan digital[9]. Masyarakat perlu diyakinkan bahwa lembaga negara mampu bekerja sama dan merespons secara cepat serta efisien terhadap ancaman siber[10]. Ketika konflik internal antar lembaga terjadi, respons menjadi terhambat dan menurunkan kredibilitas sistem keamanan[11]. Kejelasan fungsi dan batas tugas masing-masing lembaga sangat penting untuk membangun ketahanan siber yang kokoh. Tanpa landasan hukum yang kuat dan terintegrasi, sistem pertahanan siber akan terus berada dalam posisi yang rapuh.

Untuk mengatasi permasalahan tersebut, diperlukan kebijakan terpadu yang mengatur sinergi antar BSSN, Polri, dan TNI secara struktural dan operasional. Pemerintah harus menyusun regulasi dalam bentuk peraturan presiden atau protokol komando bersama untuk menghindari dualisme kewenangan. Di samping itu, perlu dibentuk sistem interoperabilitas teknologi dan pelatihan lintas institusi untuk menciptakan kolaborasi yang efektif. Dengan upaya tersebut, potensi tumpang tindih dapat ditekan dan respons terhadap ancaman dapat dilakukan dengan lebih cepat dan tepat. Penguatan koordinasi kelembagaan menjadi kunci dalam menciptakan sistem keamanan siber nasional yang tangguh dan terintegrasi.

Studi ini bertujuan untuk menganalisis secara sistematis peran dan fungsi utama dari Badan Siber dan Sandi Negara (BSSN), Kepolisian Republik Indonesia, serta Tentara Nasional Indonesia (TNI) dalam hal penanganan ancaman siber nasional. Penelitian akan memfokuskan diri pada eksplorasi titik-titik kerawanan konflik kewenangan yang mungkin terjadi akibat tumpang tindih tugas pokok dan fungsi antar lembaga. Melalui metode pendekatan hukum dan analisis kebijakan, penelitian ini akan meninjau dasar legalitas dan pelaksanaan kewenangan di lapangan. Penilaian terhadap aspek fungsional kelembagaan diharapkan dapat memberikan pemahaman yang lebih rinci tentang batas operasional masing-masing institusi. Dengan pemahaman tersebut, penelitian ini dapat memberi kontribusi dalam upaya penyusunan sistem kelembagaan yang lebih tertib dan terkoordinasi.

Di samping itu, fokus penelitian juga diarahkan pada pencarian solusi alternatif terhadap potensi sengketa yang dapat timbul di kemudian hari, terutama akibat revisi atau pembaruan Undang-Undang Polri.

---

8 Muhammad Arafat dan Alexander Tito Enggar Wirasto, "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia," *Equality : Journal of Law and Justice* 1, no. 2 (30 November 2024): 223, https://doi.org/10.69836/equality-jlj.v1i2.170.

9 Ade Irawan dkk., "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT," *JOURNAL ZETROEM* 6, no. 1 (3 April 2024): 115, https://doi.org/10.36526/ztr.v6i1.3376.

10 Jennifer Gandhi, Ben Noble, dan Milan Svolik, "Legislatures and Legislative Politics Without Democracy," *Comparative Political Studies* 53, no. 9 (Agustus 2020): 1366, https://doi.org/10.1177/0010414020919930.

11 Gabriela Ahmadi-Assalemi dkk., "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review," *Smart Cities* 3, no. 3 (13 Agustus 2020): 905, https://doi.org/10.3390/smartcities3030046.

Penelitian ini akan merumuskan langkah-langkah penyelesaian yang tidak hanya bersifat konseptual, tetapi juga dapat diterapkan dalam kebijakan kelembagaan. Tujuan utamanya adalah menciptakan kepastian hukum yang kuat dalam hal pembagian kewenangan antar lembaga negara yang terlibat dalam keamanan teknologi informasi. Kejelasan peran dan fungsi di antara lembaga sangat penting agar tidak terjadi dualisme atau kekosongan hukum. Oleh sebab itu, urgensi untuk meneliti potensi konflik kewenangan dalam perlindungan ancaman siber menjadi sangat penting dalam mendukung sistem keamanan digital yang adaptif dan terstruktur di Indonesia.

B. Metode Penelitian

Penelitian ini menerapkan metode hukum normatif yang menitikberatkan pada studi terhadap peraturan perundang-undangan dan doktrin hukum[12]. Terdapat tiga pendekatan yang digunakan, yaitu pendekatan konseptual, pendekatan perundang-undangan, dan pendekatan kasus. Pendekatan konseptual digunakan untuk memahami konsep kewenangan berdasarkan teori dari para pakar hukum serta ketentuan normatif yang berlaku[13]. Pendekatan perundang-undangan digunakan dalam menganalisis isi dari norma-norma hukum yang mengatur kewenangan lembaga-lembaga negara dalam sektor keamanan siber[14]. Sementara itu, pendekatan kasus bertujuan mengkaji preseden atau kasus hukum sebelumnya yang relevan guna memberikan refleksi kritis serta dasar evaluasi terhadap potensi konflik di masa mendatang[15].

Sumber bahan hukum utama dalam penelitian ini terdiri dari berbagai peraturan yang secara langsung mengatur peran dan kewenangan institusi terkait. Di antaranya yaitu Undang-Undang Nomor 3 Tahun 2025 sebagai perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang TNI, serta Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Juga digunakan Peraturan Presiden Nomor 28 Tahun 2021 yang mengatur tentang Badan Siber dan Sandi Negara, dan Peraturan Presiden Nomor 47 Tahun 2023 mengenai Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Bahan hukum sekunder yang digunakan meliputi buku teks mengenai administrasi publik, hukum teknologi informasi, serta artikel dan jurnal ilmiah nasional maupun internasional. Adapun bahan hukum tersier mencakup data pendukung seperti informasi media massa dan publikasi lainnya yang memiliki keterkaitan dengan fokus penelitian.

C. Pembahasan

Ancaman Siber sebagai Ancaman Serius yang di hadapi Indonesia

Indonesia telah menghadapi dua insiden serius terkait serangan siber dalam waktu dekat ini yang mencerminkan lemahnya sistem pertahanan digital nasional. Pertama, peretasan Pusat Data Nasional oleh entitas asing dengan menggunakan *ransomware* berhasil melumpuhkan sebagian besar layanan

12 Kornelius Benuf dan Muhamad Azhar, "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, no. 1 (1 April 2020): 24, https://doi.org/10.14710/gk.2020.7504.
13 Iman Jalaludin Rifa'i dkk., *Metodologi Penelitian Hukum* (Serang: Sada Kurnia Pustaka, 2023)hlm. 60.
14 Ibid.
15 Ibid.

data pemerintah[16]. Kedua, sistem SatuSehat yang digunakan untuk pelacakan informasi selama pandemi juga diretas, menimbulkan kebocoran data masyarakat. Peristiwa ini menjadi peringatan keras bahwa keamanan siber Indonesia belum berada pada posisi yang aman[17]. Ancaman semacam ini membuktikan bahwa perlindungan digital harus diperkuat secara sistematis dan strategis.

Dalam situasi ini, peningkatan perlindungan ruang digital menjadi hal mendesak yang harus dilakukan oleh pemerintah. Keamanan data tidak hanya melindungi aset digital negara, tetapi juga merupakan bentuk tanggung jawab negara terhadap warganya[18]. Kegagalan dalam menjaga data bisa menurunkan kredibilitas pemerintah dan kepercayaan publik[19]. Karena itu, pendekatan *multilapis* dan sistematis harus diterapkan agar pertahanan siber lebih kuat[20]. Implementasi strategi keamanan siber nasional harus dilandaskan pada perencanaan jangka panjang yang menyeluruh.

Kejadian peretasan dengan *ransomware* menegaskan pentingnya perubahan paradigma dalam mengelola ancaman digital[21]. Tidak cukup hanya mengandalkan perangkat lunak pertahanan; tetapi juga harus ada mekanisme cepat tanggap antar lembaga ketika insiden terjadi. Kegagalan dalam merespons secara cepat bisa memperbesar dampak serangan, baik dari sisi kerugian maupun kepercayaan publik. Oleh karena itu, sistem manajemen krisis siber nasional perlu ditata ulang dan diperkuat. Salah satu caranya adalah melalui harmonisasi tanggung jawab dan komando antar institusi yang terlibat.

Reformasi pada aspek sumber daya manusia menjadi bagian integral dari penguatan pertahanan siber nasional. Pemerintah harus berinvestasi dalam merekrut dan mengembangkan tenaga profesional di bidang teknologi dan keamanan digital. Di lingkungan BSSN, kualitas personel harus ditingkatkan agar lembaga ini mampu menjalankan fungsi secara optimal[22]. Kompetensi SDM menjadi faktor penentu apakah sebuah sistem bisa bertahan dari serangan siber yang kompleks dan masif. Penguatan kualitas internal ini harus menjadi prioritas dalam pembenahan kelembagaan.

---

16 Michelle Gabriella, "Pusat Data Nasional Jebol hingga Permintaan Tebusan Rp 131 Miliar, Ini Kilas Balik Kasusnya," *Tempo.co*, 24 Juni 2024, https://www.tempo.co/hukum/pusat-data-nasional-jebol-hingga-permintaan-tebusan-rp-131-miliar-ini-kilas-balik-kasusnya-45802.

17 Typama Randra, "Heboh PeduliLindungi Berubah Jadi Laman Judol," *news.detik.com*, 22 Mei 2025, https://news.detik.com/berita/d-7925829/heboh-pedulilindungi-berubah-jadi-laman-judol.

18 Refnaldi Kurniawan Saputra dkk., "KEAMANAN DATA PADA PENGARSIPAN SURAT MENGGUNAKAN METODE KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN SHIFT CIPHER," *ZONAsi: Jurnal Sistem Informasi* 2, no. 1 (6 Maret 2021): 62, https://doi.org/10.31849/zn.v2i1.6220.

19 Arifin La Adu, Rudy Hartanto, dan Silmi Fauziati, "HAMBATAN-HAMBATAN DALAM IMPLEMETASI LAYANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) PADA PEMERINTAH DAERAH," *JIKO (Jurnal Informatika dan Komputer)* 5, no. 3 (15 Desember 2022): 221, https://doi.org/10.33387/jiko.v5i3.5344.

20 M. Robles-Carrillo dan P. García-Teodoro, "Ransomware: An Interdisciplinary Technical and Legal Approach," ed. oleh Helena Rifà-Pous, *Security and Communication Networks* 2022 (1 Agustus 2022): 7, https://doi.org/10.1155/2022/2806605.

21 Claire C McGlave dkk., "Characteristics of Short-Term Acute Care Hospitals That Experienced a Ransomware Attack from 2016 to 2021," *Health Affairs Scholar* 1, no. 3 (4 September 2023): 4, https://doi.org/10.1093/haschl/qxad037.

22 Allisa Salsabilla Waskita dan Hasan Sidik, "Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019," *Padjadjaran Journal of International Relations* 5, no. 2 (6 Agustus 2023): 143, https://doi.org/10.24198/padjir.v5i2.41337.

Sementara itu, TNI yang kini terlibat dalam aspek keamanan siber masih membutuhkan kejelasan peran dan struktur tugas yang operasional[23]. Tanpa pedoman yang jelas, peran baru TNI dapat menimbulkan tumpang tindih kewenangan dengan lembaga lainnya. Hal ini menunjukkan perlunya penyusunan dokumen strategis yang mendefinisikan fungsi TNI dalam ruang siber secara terukur. Jika tidak ditata secara hati-hati, keberadaan TNI dalam sektor ini justru dapat menimbulkan kebingungan koordinasi. Keterlibatan militer dalam siber harus dilandasi prinsip kehati-hatian dan legalitas yang kuat.

Begitu juga dengan Polri, yang secara yuridis memiliki mandat untuk menjaga ketertiban dan menegakkan hukum di wilayah domestik, termasuk dalam dunia digital. Polri harus didukung dengan sarana, pelatihan, dan kewenangan yang jelas dalam menangani tindak pidana siber. Untuk memastikan efektivitas penanganan ancaman digital, diperlukan kerja sama sinergis antar lembaga yang dilandasi dengan regulasi yang rinci dan tegas. Ketika struktur kewenangan tidak jelas, maka efektivitas pelaksanaan kebijakan pun menjadi lemah. Oleh karena itu, penting untuk meneliti potensi konflik kewenangan dalam perlindungan ancaman siber di Indonesia agar tercipta sistem keamanan digital yang terintegrasi, efisien, dan berkelanjutan.

Kewenangan Perlindungan dari Ancaman Siber Indonesia

Konstitusi menempatkan negara sebagai pihak yang bertanggung jawab atas perlindungan keamanan dan kenyamanan setiap warga negara[24], termasuk dalam menghadapi ancaman di dunia digital. Prinsip ini merupakan bagian dari amanat negara hukum, di mana semua kebijakan dan tindakan harus berlandaskan norma hukum[25]. Dalam hal ini, BSSN, TNI, dan Polri serta Komdigi memiliki peran masing-masing dalam mengelola dan menangani isu keamanan siber. Ketiga institusi tersebut memiliki fungsi yang telah diatur secara khusus agar saling mendukung dalam menghadapi gangguan di ruang siber. Tugas mereka merupakan bagian integral dari strategi nasional dalam menjaga stabilitas dan keamanan digital negara.

Dalam perspektif teori negara hukum, setiap tindakan negara, termasuk dalam menghadapi kejahatan siber, wajib tunduk pada ketentuan hukum yang berlaku[26]. Perlindungan terhadap sistem digital nasional merupakan perwujudan konkret dari tanggung jawab negara terhadap warganya[27]. BSSN berperan dalam koordinasi dan teknis pengamanan[28], TNI bertugas untuk

---

23 Dinanda Diadeska Diara, "Strategi Keamanan Siber Korea Selatan," *Jurnal Indonesia Sosial Sains* 1, no. 4 (21 November 2020): 293, https://doi.org/10.36418/jiss.v1i4.44.

24 Christian Immanuel Situmorang dkk., "Pentingnya Hukum yang Tegas dalam Mempertahankan Hak Asasi Manusia: Perspektif Konstitusi: (The Importance of Strict Law in Defending Human Rights: A Constitutional Perspective)," *Journal Customary Law* 1, no. 2 (8 Mei 2024): 2, https://doi.org/10.47134/jcl.v1i2.2427.

25 Selfianus Laritma dan Ahmad Rosidi, *Teori-Teori Negara Hukum (Perspektif Kewenangan Mahkamah Agung dalam Melakukan Pengujian Peraturan Perundang-Undangan di Bawah Undang-Undang)* (Jakarta: Kencana, 2024), hlm 242.

26 Jarot Digdo Ismoyo dkk., *Teori Negara Hukum Modern* (Jambi: Sonpedia Publishing Indonesia, 2025), hlm 42.

27 Arief Bakhtiar Darmawan, Kholifatus Saadah, dan I Putu Arya Aditia Utama, "Kedaulatan Negara dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook dan Google," *Jurnal Hubungan Internasional* 16, no. 1 (13 Juli 2023): 216, https://doi.org/10.20473/jhi.v16i1.38971.

28 Ahmad Budiman, "OPTIMALISASI PERAN BADAN SIBER DAN SANDI NASIONAL," *Majalah Info Singkat Pemerintahan Dalam Negeri* 9, no. 12 (Juni 2017): 17.

ancaman siber lintas batas atau eksternal, dan Polri berwenang dalam penegakan hukum terhadap pelaku di dalam negeri[29]. Ketiga lembaga tersebut diberikan porsi kewenangan yang berbeda namun saling melengkapi. Maka, penting untuk memastikan pelaksanaan tugas masing-masing dilakukan secara terkoordinasi agar tidak menimbulkan konflik atau kekosongan peran dalam sistem keamanan nasional.

1. Kewenangan BSSN pada Keamanan Siber

Secara historis, BSSN dibentuk sebagai reaksi pemerintah atas meningkatnya ancaman terhadap sistem digital nasional. Lembaga ini resmi berdiri melalui Perpres No. 53 Tahun 2017, dengan menyatukan fungsi Lembaga Sandi Negara dan Direktorat Keamanan Informasi Kementerian Kominfo[30]. Tujuannya adalah menghindari fragmentasi pengelolaan keamanan siber yang sebelumnya tidak terkoordinasi dengan baik[31]. Pembentukan ini diperkuat dengan Perpres No. 28 Tahun 2021 yang menata ulang struktur dan kewenangan BSSN agar lebih efektif. Sejak saat itu, BSSN menjadi lembaga utama dalam mengoordinasikan keamanan dan pertahanan siber di Indonesia.

Dalam kerangka konseptual, BSSN merupakan badan negara yang bertanggung jawab menjaga keamanan digital dan integritas ruang siber nasional[32]. Tugasnya mencakup penyusunan kebijakan, pelaksanaan teknis, serta peningkatan kesadaran publik mengenai risiko siber. Selain sebagai pelaksana teknis, BSSN juga bertindak sebagai lembaga koordinatif yang menjembatani kerja sama antar sektor pemerintah dan swasta[33]. Fungsi strategisnya adalah menjaga keamanan data nasional dan menciptakan lingkungan digital yang aman dan berkelanjutan. Posisi ini menjadikan BSSN sebagai pengawal utama kedaulatan dan perlindungan siber di Indonesia.

Dalam aspek regulatif, kewenangan BSSN ditetapkan melalui Peraturan Presiden Nomor 28 Tahun 2021 yang memuat tugas pokok dan fungsi lembaga ini secara rinci. BSSN berwenang menyusun kebijakan keamanan siber nasional, mengawasi sistem elektronik strategis, dan merespons insiden siber yang terjadi di berbagai sektor[34]. Lembaga ini juga memiliki peran dalam pemberian sertifikasi keamanan informasi serta

---

29 Jansen Chandra, Vincent Tanaka, dan Ricky Banke, "Peran Interpol dalam Menangani dan Menanggulangi Kejahatan Siber di Indonesia," *PESHUM: Jurnal Pendidikan,Sosial dan Humaniora* 4, no. 3 (17 April 2025): 4716, https://doi.org/10.56799/peshum.v4i3.9028.

30 Apryan Anggara Pratama dan Muhammad Ruhly Kesuma Dinata, "Hacker Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data," *Jurnal Hukum Magnum Opus* 6, no. 1 (27 Februari 2023): 19, https://doi.org/10.30996/jhmo.v6i1.8293.

31 Muhammad Rafi Shiddique dan Mansur Juned, "Human Capital Development for Cybersecurity: Examining BSSN's Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020)," *Journal of Social and Political Sciences* 6, no. 4 (30 Desember 2023): 218, https://doi.org/10.31014/aior.1991.06.04.457.

32 Afifah Fidina Rosy, "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security," *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan* 1, no. 2 (22 Juli 2020): 119, https://doi.org/10.54144/govsci.v1i2.12.

33 Muhammad Arafat dan Alexander Tito Enggar Wirasto, "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia," *Equality : Journal of Law and Justice* 1, no. 2 (30 November 2024): 231, https://doi.org/10.69836/equality-jlj.v1i2.170.

34 Herni Ramayanti dan Arief Fahmi Lubis, "Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional," *Jurnal Hukum dan HAM Wara Sains* 2, no. 9 (29 September 2023): 905, https://doi.org/10.58812/jhhws.v2i09.672.

pembinaan terhadap unit tanggap insiden (CSIRT)[35]. BSSN menjalankan fungsinya melalui kerja sama lintas lembaga dan sektor sebagai bentuk pendekatan kolaboratif. Kewenangan tersebut memperkuat posisi BSSN sebagai otoritas sentral dalam membangun ketahanan siber nasional yang adaptif dan integratif.

2. Kewenangan TNI pada Keamanan Ancaman Siber

Awalnya, peran TNI dalam menangani ancaman siber belum secara tegas disebutkan dalam regulasi yang berlaku. UU Nomor 34 Tahun 2004 tentang TNI yang mengalami perubahan Undang-Undang Nomor 3 Tahun 2025 hanya menyebutkan tugas umum dalam menjaga pertahanan negara dari berbagai jenis ancaman. Namun, seiring berkembangnya bentuk ancaman modern seperti serangan digital, peran TNI perlu diperluas agar dapat merespons dinamika pertahanan yang semakin kompleks. Maka, perubahan regulasi menjadi hal yang mendesak agar TNI dapat secara legal terlibat dalam pengamanan ruang siber. Pembaruan ini memberikan landasan hukum bagi keterlibatan militer dalam bidang yang sebelumnya hanya didominasi oleh lembaga sipil.

Penyesuaian regulasi tersebut diwujudkan melalui UU Nomor 3 Tahun 2025 yang merevisi UU TNI sebelumnya. Dalam ketentuan baru ini, TNI diberikan wewenang untuk menangani ancaman siber sebagai bagian dari tugas pertahanan negara secara menyeluruh[36]. Perluasan ini menandai pengakuan bahwa ruang siber kini telah menjadi bagian dari ranah strategis yang harus diamankan oleh unsur militer. Negara memandang keterlibatan TNI sebagai bagian penting dari strategi pertahanan digital nasional. Kewenangan ini memungkinkan TNI turut serta dalam pengamanan sistem elektronik strategis yang rentan terhadap serangan dari luar negeri.

Secara konseptual, ancaman digital dianggap sebagai salah satu bentuk serangan non-konvensional yang bisa berdampak sistemik terhadap keamanan negara[37]. Karena itu, tugas TNI diperluas agar bisa merespons, mengantisipasi, dan menghalau potensi serangan siber dari luar yang membahayakan kedaulatan negara. Pelibatan ini juga menekankan kerja sama antara TNI, BSSN, dan Polri untuk menciptakan sistem pertahanan digital yang saling melengkapi. Dalam posisi ini, TNI menjadi garda depan dalam menghadapi ancaman siber lintas batas yang bersifat strategis dan sensitif. Dengan demikian, peran TNI dalam keamanan digital merupakan bagian integral dari pertahanan nasional era modern.

Dampak dari pelibatan TNI dalam keamanan siber mencakup kebutuhan restrukturisasi kelembagaan dan peningkatan keahlian personel dalam bidang teknologi digital[38]. TNI

---

35 Ricky Febriansyah dan Ana Husnayanti, "Keamanan Sistem Informasi Pemilu Melalui Computer Security Incident Response Team (Csirt) Pemilu Serentak 2024," *JIPOSSTER: Jurnal Ilmu Politik dan Studi Sosial Terapan* 3, no. 4 (t.t.): 67.

36 Pasal 7 ayat (2) Undang-Undang No. 3/2025 perubahan Undang-Undang No. 34/2004 tentang Tentara Nasional Indonesia dijelaskan pada angka 15 mengenai tugas dan wewenang mengenai perlindungan dari ancaman siber.

37 Washington Okori dan Sarah Buteraba, "Cyber Security Exploits and Management in Telecommunication Companies: The Case of Uganda," *Journal of Computer Science and Technology Studies* 6, no. 4 (5 Oktober 2024): 74, https://doi.org/10.32996/jcsts.2024.6.4.10.

38 Elena Polevaya dan Irina Shustova, "The Impact of Digitalization on Organizational Management Structures," ed. oleh V. Pukhkal dan S. Uvarova, *E3S Web of Conferences* 458, no. 04007 (2023): 1–8, https://doi.org/10.1051/e3sconf/202345804007.

perlu mengembangkan satuan atau unit khusus yang menangani operasi siber secara profesional dan terfokus. Untuk menghindari konflik dengan lembaga lain, kerja sama yang jelas dan mekanisme koordinasi harus dibangun[39]. Selain itu, pengawasan dari sisi hukum dan kebijakan sipil tetap dibutuhkan untuk memastikan keterlibatan militer sesuai dengan prinsip negara demokratis[40]. Oleh karena itu, keterlibatan TNI dalam perlindungan siber harus dilakukan secara tepat, proporsional, dan dalam kerangka hukum yang transparan.

3. Kewenangan Kepolisian Republik Indonesia dalam Penegakan Hukum Kejahatan Siber

Kepolisian Republik Indonesia (Polri) memiliki otoritas untuk menangani kejahatan siber sejak tahapan awal berupa penyelidikan[41]. Berdasarkan Undang-Undang Nomor 2 Tahun 2002, Polri diberi mandat untuk menjaga ketertiban dan keamanan, termasuk menanggulangi kejahatan berbasis teknologi[42]. Dalam tahap penyelidikan, Polri melakukan pengumpulan informasi awal terhadap aktivitas digital yang diduga melanggar hukum, seperti akses ilegal atau manipulasi data. Kegiatan ini bertujuan untuk memastikan bahwa ada dasar hukum dan bukti permulaan yang cukup sebelum melangkah ke tahap penyidikan. Dalam pelaksanaannya, penyelidikan memanfaatkan perangkat dan metode digital guna menelusuri jejak kejahatan di ruang siber[43].

Setelah penyelidikan menghasilkan bukti awal yang kuat, Polri melanjutkan proses ke tahap penyidikan untuk mengusut lebih dalam keterlibatan pelaku kejahatan. Proses penyidikan memberikan kewenangan kepada Polri untuk menyita perangkat elektronik, memanggil saksi, dan melakukan penggeledahan sesuai dengan prosedur dalam KUHAP[44]. Penyidikan juga mencakup pelacakan asal-usul serangan, jaringan pelaku, serta identifikasi motif tindak pidana yang dilakukan[45]. Dalam kasus yang

---

39 Siska Habibah dkk., "IMPLEMENTASI KONSEP CHECK AND BALANCE PETER L. STRAUSS DALAM SISTEM KELEMBAGAAN INDONESIA," *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 1 (25 Januari 2025): 359–67, https://doi.org/10.59141/cerdika.v5i1.2431.

40 Tiara Saskia Maharani, "Law Enforcement Regarding Human Rights According to Positive Law in Indonesia," *Journal of Strafvordering Indonesian* 1, no. 1 (12 Maret 2024): 1–5, https://doi.org/10.62872/n1f51e68.

41 Madinah Mokobombang, Zulfikri Darwis, dan Sabil Mokodenseho, "Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital," *Jurnal Hukum dan HAM Wara Sains* 2, no. 06 (28 Juni 2023): 517–25, https://doi.org/10.58812/jhhws.v2i6.447.

42 Dalam Undang-Undang Kepolisian Republik Indonesia, tidak ditemukan ketentuan yang secara eksplisit menetapkan bahwa Polri memiliki tugas khusus menangani kejahatan siber. Meski demikian, kewenangan Polri dalam menangani tindak pidana siber muncul melalui peran mereka sebagai penyidik, khususnya terhadap pelanggaran yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Dalam praktiknya, Polri memiliki otoritas untuk melakukan penyidikan terhadap pelaku kejahatan digital berdasarkan amanat undang-undang tersebut. Ini berarti bahwa meskipun tidak dirinci dalam UU Kepolisian, kewenangan tersebut bersifat melekat berdasarkan ketentuan hukum lainnya. Dengan demikian, peran Polri dalam menanggulangi kejahatan siber bersifat interdependen dengan regulasi sektoral yang mengatur substansi kejahatannya.

43 Imas Novita Juaningsih dkk., "Rekonsepsi Lembaga Pengawas terkait Perlindungan Data Pribadi oleh Korporasi sebagai Penegakan Hak Privasi berdasarkan Konstitusi," *SALAM: Jurnal Sosial dan Budaya Syar-i* 8, no. 2 (5 Maret 2021): 469–86, https://doi.org/10.15408/sjsbs.v8i2.19904.

44 Arthur Simada dkk., "Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain)," *Locus Journal of Academic Literature Review* 3, no. 4 (29 April 2024): 349–61, https://doi.org/10.56128/ljoalr.v3i4.314.

45 Benoît Dupont dan Chad Whelan, "Enhancing Relationships between Criminology and Cybersecurity," *Journal of Criminology* 54, no. 1 (Maret 2021): 76–92, https://doi.org/10.1177/00048658211003925.

kompleks, Polri dapat bekerja sama dengan lembaga lain seperti BSSN dan Kominfo untuk memperoleh data teknis dan dukungan keahlian. Tujuan akhir dari tahap ini adalah menyusun berkas perkara yang lengkap untuk diajukan ke jaksa penuntut umum.

Setelah berkas perkara dinyatakan lengkap, Polri memiliki tanggung jawab untuk menyerahkan kasus tersebut kepada kejaksaan guna dilanjutkan ke proses penuntutan. Seluruh barang bukti, dokumen hukum, dan hasil penyidikan diserahkan sebagai bagian dari pelimpahan perkara. Dalam proses ini, Polri tetap berperan sebagai pendukung teknis, seperti menghadirkan saksi ahli atau memberikan keterangan tambahan yang dibutuhkan di persidangan[46]. Kolaborasi antara Polri dan kejaksaan menjadi kunci untuk memastikan kejahatan siber dapat ditangani secara tuntas melalui proses hukum yang sah. Oleh karena itu, kewenangan Polri tidak hanya terbatas pada penyelidikan, tetapi mencakup keseluruhan rantai penegakan hukum hingga kasus diproses di pengadilan.

4. Kewenangan Kementerian Komunikasi dan Digitalisasi (KOMDIGI)

Dalam ranah keamanan siber nasional, keberadaan KOMDIGI pada hakikatnya memegang peran startegis sebagai bagian dari regulator dan pengawas utama penyelenggaraan sistem elektronik Indonesia dengan tupoksi dan fungsi untuk melakukan penetapan kebijakan di bidang komunikasi dan infromatika, dengan cakupan terkait pengembangan infrastruktur digital seperti aplikasi pemerintahan yang selaras dengan penerapan *e-government* di berbagai tingkat lembaga, pengelolaan data dan informasi, perlindungan informasi public, serta pengembangan infrastruktur telekomunikasi.

Berdasarkan ketentuan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024 yang memberikan perluasan terhadap peran KOMDIGI terutama dalam pengaturan dan pengawasan ruang siber.

Salah satu yang menjadi ketentuan penting landasan kewenangan KOMDIGI termuat dalam ketentuan Pasal 40 ayat (2a) dan (2b). dalam ketentuan ayat (2a) memberikan penegasan kewajiban bagi pemerintah untuk melindungi kepentingan umum dari segala jenis gangguan akibat penyalahgunaan infromasi elektronik dan transaksi elektronik yang menggangu ketertiban umum, sementara ayat (2b) memberikan kewenangan kepada pemerintah untuk melakukan pemutusan akses atau memperintahkan penyelengara sistem elektronik (PSE) untuk melakukan pemutusan terhadap akses informasi elektronik atau dokumen elektronik yang bermuatan melanggar hukum. Berdasarkan ketentuan ini secara tidak langsung memberikan letigimasi bagi KOMDIGI untuk melakukan pemblokiran konten illegal dan membatasi konten iligal.

Kewenangan KOMDIGI ini juga dipertegas dalam ketentuan Pasal 33 PP Nomor 71 Tahun 2019 terkait kewenangan pengawasan yang mencakup pemantauan, pengendalian, pemeriksaan, penelurusan, dan pengamanan. Selain itu, Pasal 30 hingga 32 PP Nomor 71 Tahun 2019 memberikan kewenangan bagi

[46] Hafiz Pratama S Nawawi, Carrudin, dan Dadang Yusup, "ANALISIS PENEMUAN BARANG BUKTI DIGITAL MELALUI REKAMAN SUARA MENGGUNAKAN PRAAT DENGAN METODE AUDIO FORENSIK," *CyberSecurity dan Forensik Digital* 4, no. 2 (19 April 2024): 96–103, https://doi.org/10.14421/csecurity.2021.4.2.2638.

KOMDIGI untuk menetapkan standar kelaikan sistem elektronik guna memastikan aspek keamanan teknis.

Sebagaimana peran dan fungsinya dalam siber. KOMDIGI dapat melakukan kerjasama dengan BSSN terutama pada aspek regulasi dan pengembangan infrastruktur, namun lebih berfokus pada kolaborasi teknis penguatan keamanan siber. Kedudukan KOMDIGI sebagai regulator menjadikan penghubung antara kebijakan publik, swasta, dan otoritas teknis seperti BSSN, sehingga walaupun dalam hal ini KOMDIGI tidak menjalankan fungsi operasiona pertahanan siber, kementerian ini menjadi pintu utama bagi penetapan standar, pengawasan, dan penegakan administratif di ruang digital.

Sedangkan BSSN dapat berperan sebagai pelaksana audit teknis, melakukan upaya mitigasi insiden, dan pengamanan pada infrastruktur. Selain itu, pada aspek koordinasi atau hubungan dengan lembaga lain, menurut hikmat penulis, KOMDIGI dapat melakukan kerjasama dengan TNI. Hal ini sebagaimana pernyataan Menkomdigi terhadap revisi UU TNI, diharapkan dapat meningkatkan kesiapan prajurit TNI dalam menghadapi ancaman mencakup ancaman siber. Mesikipun pada dasarnya kewenangan KOMDIGI tidak secara langsung bersingungan dengan pertahanan siber militer, namun dengan melakukan pemantauan terutama yang diperoleh dari penyelenggaraan sistem elektronik dapat dimanfatkan oleh TNI sebagai bahan data intelijen apabila terdapat ancaman terutama berasal dari luar negeri.

Pada konteks kewenangan KOMDIGI dengan Polri. KOMDIGI dapat berperan pada tahap administrasi dan pelaporan insiden ancaman siber, sedangkan Polri berwenang untuk penanganan pada tahap penyidikan dan penegakan hukum.

Namun, terdapat sejumlah permasalahan yang perlu menjadi bahan pertimbangan dalam rangka penguatan kewenangan KOMDIGI, terutama pada peran dan fungsinya, yaitu terkait dengan kewenangan KOMDIGI yang dapat melakukan pemutusan akses dan penghapusan konten yang kerap menjadi sumber perdebatan, terutama pada aspek perlindungan HAM, kebebasan berekspresi, dan penerapan prinsip *due process* itu sendiri.

Tabel. I Pembagian lembaga negara yang berwenang dalam penanganan ancaman siber di Indonesia

Lembaga	Tugas	Upaya
BSSN	Menganalisa dan mencegah ancaman siber dari luar maupun dalam.	Preventif
TNI	Melindungi dari ancaman siber luar wilayah negara.	Defensif
Polri	Menegakkan hukum dan melakukan tahap pemeriksaan, penyelidikan, penyidikan, sampai penahan dengan di limpahkan kepada kejaksaan.	Represif
KOMDIGI	regulator dan pengawas utama penyelenggaraan sistem elektronik Indonesia	Represif

Sumber: diolah sendiri oleh penulis.

Ius Constituendum dalam Sengketa Kewenangan pada Ancaman Siber di Indonesia

Indonesia saat ini tengah menghadapi situasi darurat siber akibat tingginya intensitas serangan digital yang mengganggu berbagai sektor vital. Serangan tersebut memperlihatkan

lemahnya sistem keamanan digital nasional yang belum siap menghadapi kompleksitas ancaman global. Situasi ini mengindikasikan belum terbangunnya koordinasi dan integrasi yang solid di antara institusi yang menangani keamanan siber. Untuk menghadapi kondisi tersebut, pemerintah perlu mengambil langkah strategis dan komprehensif guna memperkuat pertahanan siber secara menyeluruh. Salah satu solusi krusial adalah dengan memperjelas batas dan kewenangan dari masing-masing lembaga yang memiliki peran dalam keamanan siber[47].

Penambahan fungsi Tentara Nasional Indonesia (TNI) dalam menangani ancaman siber merupakan bentuk respons kebijakan yang signifikan. Kewenangan ini ditetapkan dalam Undang-Undang Nomor 3 Tahun 2025 sebagai amandemen dari UU TNI sebelumnya. Meski demikian, tidak ada kejelasan teknis mengenai bentuk pelaksanaan tugas tersebut, terutama dalam membedakan antara ancaman siber eksternal dan internal. Tanpa pengaturan pelaksana yang rinci, pelaksanaan tugas TNI dalam ruang siber berpotensi menimbulkan konflik dengan lembaga lain. Maka, diperlukan peraturan turunan yang mendetail agar pelaksanaan peran TNI di domain siber berjalan efektif dan sesuai kerangka hukum nasional.

Sementara itu, peran Badan Siber dan Sandi Negara (BSSN) sebagai lembaga khusus keamanan siber saat ini masih terbatas pada kegiatan analitis dan koordinatif. Padahal, dalam situasi ancaman digital yang terus berkembang, BSSN semestinya diperkuat menjadi lembaga pelaksana teknis utama dalam merancang dan melindungi sistem digital nasional. Perluasan fungsi ini harus disertai dengan peningkatan otoritas dan wewenang yang memungkinkan BSSN memimpin strategi pertahanan siber nasional. Reformasi kelembagaan juga penting untuk menyesuaikan fungsi BSSN dengan tantangan zaman. Salah satunya adalah melalui penguatan SDM dengan keahlian tinggi di bidang teknologi informasi.

Rekrutmen sumber daya manusia di BSSN harus diarahkan untuk mengakomodasi tenaga muda yang memiliki potensi dan minat dalam bidang keamanan siber. Peningkatan kompetensi internal merupakan syarat mutlak agar BSSN dapat bertransformasi menjadi institusi pertahanan digital yang adaptif. Kolaborasi dengan dunia akademik dan industri teknologi menjadi penting untuk membangun ekosistem keamanan digital nasional yang berkelanjutan. Rekrutmen yang berbasis keahlian juga harus disertai pelatihan berkelanjutan dan sertifikasi profesional. Dengan langkah tersebut, BSSN dapat berperan sebagai lembaga yang tidak hanya mengatur, tetapi juga merancang sistem keamanan digital secara langsung.

Di sisi lain, Kepolisian Republik Indonesia (Polri) memainkan peran vital dalam proses penegakan hukum terhadap tindak pidana siber, namun belum memiliki dasar hukum khusus terkait upaya perlindungan preventif. Kewenangan Polri saat ini masih terbatas pada penyidikan kejahatan digital berdasarkan Undang-Undang ITE dan belum mencakup aspek pertahanan siber nasional. Oleh karena itu, diperlukan penguatan regulasi yang secara eksplisit memberi wewenang kepada Polri untuk bertindak dalam perlindungan sistem digital dalam negeri. Selain itu, Polri perlu mengembangkan metode penanganan

[47] Sabri Balafif, "Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework," *Jurnal Informatika: Jurnal Pengembangan IT* 8, no. 3 (10 November 2023): 291–301, https://doi.org/10.30591/jpit.v8i3.5662.

kejahatan siber yang lebih inovatif, termasuk pemanfaatan teknologi forensik digital. Dukungan regulasi dan sumber daya menjadi elemen penting agar fungsi Polri dalam ruang siber dapat berjalan optimal.

Untuk menghindari konflik kewenangan di antara BSSN, TNI, dan Polri, perlu dirumuskan kerangka kerja nasional yang membagi tugas secara tegas, transparan, dan operasional. Kerangka ini harus mengatur batas wilayah kewenangan masing-masing lembaga agar tidak terjadi tumpang tindih dalam pelaksanaan tugas. Berikut adalah tabel perbandingan fungsi utama ketiga institusi tersebut:

Selain itu, bentuk penguatan sistem keamanan siber di Indonesia dapat dilakukan dengan merujuk pada pratik dan kebijakan yang diterpakan di negara lain sebagai bahan perbandingan terkhusus terkait aspek tugas dan wewenang lembaga serta mekanisme koordinasi antarinstansi yang berwenang.

Sebagai contoh, perbandingan dapat dilakukan dengan melihat pada negara Singapura, melalui Cybersecurity Act 2018[48], menetapkan kerangka hukum yang kompeherensif terkait pengelolaan keamanan siber, yang mencakup penetapan otorutas pusat, pelindungan *critical information Infrastructure* (CII), kewajiban

Tabel II. Solusi alternatif untuk penanganan kejahatan siber di Indonesia

Lembaga	Peran Strategis	Cakupan Tugas	Peraturan
BSSN	Pengelolaan, regulasi, dan pengawasan keamanan siber nasional.	Seluruh sektor infrastruktur siber.	Perpres No. 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.
TNI	Pertahanan negara terhadap serangan siber eksternal.	Ancaman siber dari luar negeri.	UU No. 3 Tahun 2025 perubahan atas UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia.
Polri	Penegakan hukum dan penyidikan terhadap kejahatan digital.	Ruang domestik dan kejahatan internal.	UU No. 2 Tahun 2002 tentang Kepolisian Republik Indonesia & UU ITE
Komdigi	Regulator	Perumus Regulatur Ruang domestik dan kejahatan internal.	Peraturan Presiden Republik Indonesia Nomor 22 Tahun 2023

Sumber: diolah sendiri oleh penulis.

Pembagian peran yang jelas dan sinergis antara ketiga lembaga ini akan menjadi fondasi penting bagi sistem keamanan siber Indonesia yang efektif, responsif, dan berkelanjutan di tengah ancaman digital yang semakin kompleks.

pelaporan insiden, mekanisme investigasi, serta koordinasi antarinstansi secara terpusat.

Pada kontes otoritas dan kewenangan diatur dalam Pasal 3 hingga 5 yang menetapkan *Commissioner of Cybersecurity* sebagai pejabat

[48] Lihat pada Cybersecurity Act 2018 (No.9 of 2018)

tertinggi di bawah *Cyber Security Agency of Singapore (CSA),* dengan kewenangan penuh untuk melakukan penetapan kebijakan, mengeluarkan arahaan keamanan siber, dan menunjuk petugas bagian investigasi. Selanjutnya Pasal 6 memberikan penegasan terkait kewenangan *Cyber Security Agency of Singapore (CSA*), untuk melakukan penetapan standar teknis dan prosedur keamanan siber yang wajib dipatuhi oleh *operator Critical Information Infrastructure*, sedangkan pada Pasal 7 memberikan penghaturan terkait hak *Cyber Security Agency of Singapore (CSA),* untuk melakukan inspeksi dan audit terhadap sistem CII, termasuk pada aspek pemberian akses terhadap data. Merujuk pada pengaturan ini memberikan sentralisasi otoritas yang menutup adanya potensi tumpang tindih kewenangan dan berada dalam satu pengawas, dari ketentuan ini menjadi pertimbangan bagi Indonesia untuk memeperkuat kedudukan dan kewenangan BSSN sebagai otoritas pusat dengan kewenangan berupa mandat.

Selanjutnya dalam Pasal 14 dan Pasal 15 memberikan ketentuan kewajiban bagi *critical information Infrastructure (CII)* untuck melaporkan adanya inseiden acaman siber dalam jangka waktu tertentu, sedangkan dalam ketentuan Pasal 19, Pasal 20, dan Pasal 21 memberikan kewenangan *Cyber Security Agency of Singapore (CSA)* untuk mengeluarkan *incident response directions* dan *remedial measures* yang bersifat mengikat. Adanya mekanisme yang mempersingkat waktu respon dan memastikan koordinasi terpusat. Sedangkan Indonesia hingga saat ini pelaporan ancaman siber masih bersifat pada sektiral tanpa adanya kodifikasi kerangka hukum yang terintegrasi.

Selanjutnya, dalam Pasal 36, Pasal 37 dan Pasal 38 memberikan pengaturan terkait perturakan informasi antara *Cyber Security Agency of Singapore (CSA),* Kepolisian, Regulator sektor, dan *operator Critical Information Infrastructure.* Sedangkan Pasal 39 memberikan pengaturan perlindungan kerahasiaan informais startegis yang mendasar pada prinsip *single point of contact* yang diatur secara eskplisit. Pengaturan ini bertujuan untuk mecegah adanya absurditas kewenangan dan koordinasi antar lembaga tersebut. Merujuk pada ketentuan ini, Indonesia dapat mengadob ketentuan negara Singapura dengan menempatkan BSSN sebagai simpul koordinasi tunggal dalam keamanan siber, sebagaimana peran *Cyber Security Agency of Singapore (CSA*).

Selain itu, salah satu langkah strategis yang dapat diadobsi untuk mengatasi permasalahan terhadap tumpang tindah kewenangan antara lembaga dengan melalui pembentukan Rancangan Undang-Undang Keamanan Siber (RUU KKS). Pembentukan RUU ini didorong oleh kebutuhan akan kerangkan hukum yang kompherensif untuk memperkuat ketahanan siber, melindungi data nasional serta penyelarasan terhadap kebijakan keamanan siber nasional dengan standard dan pratik internasional.[49] Dengan muatan pengaturan terkait tata kelola keamanan siber, ketahanan, dan perlindungan siber di Indonesia, meliputi kegiatan deteksi, identifikasi, perlindungan, penanggulangan, pemulihan, pemantauan, hingga pengendalian terhadap berbagai objek yang menjadi sasaran pengamanan ruang siber.[50]

[49] Naskah Akademik Rancangan Undang-Undang Keamanan dan Ketahanan Siber.
[50] Muhammad Arief, "Urgensi Regulasi Ketahanan dan Keamanan Siber dalam Undang-Undang ITE", *Julia Jurnal Litigasi Amsir,* Special Issue, 2022. https://journalstih.amsir.ac.id/index.php/julia/article/view/127

RUU KKS juga mengatur penerapan sanksi administratif selain sanksi pidana, sanksi ini secara bertahap mulai dari teguran, pembekuan atau pemblokiran sementara, pencabutan permanen izin akses maupun operasional sistem elektronik, hingga pengenaan denda sebagai instrumen penegakan kepatuhan bagi pelaku atau penyelenggara keamanan siber serta penyedia jasa terkait. Mekanisme ini dilengkapi dengan jaminan hak untuk mengajukan upaya pembelaan, yang pengaturannya dirinci lebih lanjut dalam peraturan pelaksana.

Selain itu, salah satu tujuan utama RUU KKS ini untuk memperkuat peran dan fungsi dari BSSN sebagai otoritas nasional yang memiliki mandat penuh dalam penyelenggaraan keamanan siber dengan pertanggungjawaban langsung kepada Presiden.

RUU KKS mengadopsi konsep Public-Private Partnership yang menempatkan keamanan siber sebagai tanggung jawab bersama antara pemerintah dan sektor swasta. Pendekatan ini didorong oleh fakta bahwa sebagian besar Cyber Critical Infrastructure di Indonesia dimiliki oleh pihak swasta. Dengan BSSN sebagai *focal point*.

RUU KKS menegaskan urgensi kolaborasi serta keterpaduan aktivitas antar pemangku kepentingan pemerintah yang memiliki fungsi di bidang siber, termasuk TNI, Polri, Kejaksaan, Badan Intelijen Negara, Kementerian Komunikasi dan Informatika, serta instansi terkait lainnya. Hal ini dilatarbelakangi adanya ubungan antara BSSN, KOMDIGI, TNI, Polri, BIN, Kejaksaan, serta berbagai lembaga non-pemerintah memiliki potensi strategis untuk membangun sinergi yang kuat dalam memperkuat keamanan siber nasional. Namun, ketiadaan mekanisme koordinasi yang tegas berisiko menimbulkan tumpang tindih kewenangan yang dapat mengurangi efektivitas penanganan ancaman siber.

Sehingga terhadap kerangka RUU KKS dapat memberikan penawaran desain kelembagaan diarahkan untuk memperjelas pembagian peran antaraktor utama. BSSN diposisikan sebagai otoritas pusat (single authority) yang menetapkan kebijakan dan standar teknis, mengakreditasi dan mensertifikasi kompetensi serta perangkat, melakukan audit keamanan terhadap Critical Information Infrastructure (CII), memimpin incident response nasional, dan mengelola cyber threat intelligence lintas-sektor, termasuk melakukan pengujian/penetrasi sah sebagai bagian dari proactive defense. Penguatan BSSN di tingkat undang-undang diperlukan agar mampu mengoordinasikan kementerian/lembaga yang lahir dari UU serta sektor privat pemilik CII, karena Perpres saja tidak memadai untuk memaksa kepatuhan lintas-sektor. TNI berperan pada domain pertahanan siber, khususnya kontra-ancaman lintas batas, strategic cyber operations, dan perlindungan kedaulatan digital, dengan batas operasional yang jelas untuk menghindari tumpang tindih dengan penegakan hukum domestik, serta mekanisme tasking saat national cyber emergency yang sesuai prinsip hukum demokratis dan kontrol sipil. Polri memegang fungsi represif melalui penyelidikan, penyidikan, forensik digital, dan penindakan pelaku di yurisdiksi domestik, dengan keterkaitan kewajiban pelaporan insiden dan pelestarian barang bukti digital ke chain of custody guna memastikan due process. Sementara itu, KOMDIGI sebagai regulator sektor digital dan PSE bertanggung jawab atas standardisasi kelaikan sistem elektronik, pengawasan, dan penegakan administratif, termasuk pemutusan akses konten ilegal sesuai UU ITE/PP 71/2019,

yang kewenangannya harus terintegrasi secara prosedural dengan BSSN, Polri, dan TNI agar data atau insiden dari PSE dapat segera diolah menjadi actionable intelligence.

Oleh karena itu, keberadaan RUU Keamanan dan Ketahanan Siber menjadi krusial sebagai landasan hukum untuk menjamin efisiensi, akuntabilitas, dan keterpaduan dalam tata kelola keamanan siber nasional.

Pembaruan pada keamanan siber tentunya sejalan dengan hukum transformatif yaitu kerangka pemikiran yang menawarkan pendekatan hukum baru untuk merespons kemajuan teknologi secara lebih dinamis dan adaptif. Prinsipnya menegaskan bahwa hukum tidak hanya bertugas menciptakan ketertiban, keadilan, kepastian, dan kemanfaatan, tetapi juga berperan sebagai penggerak perubahan positif dalam menghadapi perkembangan teknologi dan transformasi digital. Dalam konteks keamanan siber, pendekatan ini berarti regulasi tidak cukup sekadar mengatur dan membatasi, melainkan harus proaktif mendorong inovasi, memperkuat ketahanan infrastruktur digital, serta memastikan perlindungan hak-hak masyarakat di ruang siber. Fenomena ancaman siber yang semakin kompleks menuntut para regulator untuk mengadopsi prinsip hukum transformatif, sehingga kebijakan yang dihasilkan mampu menjawab dinamika ancaman dan peluang di era digital secara efektif dan berkelanjutan.[51] Sebagaimana diasampaikan oleh Ahmad M Ramli memberikan penekanan bahwa hukum sesungguhnya bukan hanya untuk aturan dan regulasi, namun juga sebagai infrastrutur yang memungkinkan bangsa dapat beradaptasi dan berkembang di era digital yang penuh dengan perubahan pesat.[52]

Selain itu, diperlukannya pemahaman terhadap perbedaan konseptual antara keamanan siber (*cybersecurity*) dan ketahanan siber (*cyberresilience*) harus menjadi pijakan utama dalam membangun kerangka hukum nasional dalam RUU KKS. *Cybersecurity* menekankan aspek pencegahan, deteksi, dan proteksi, sedangkan *cyberresilience* menekankan kemampuan sistem untuk tetap berfungsi dan pulih pasca serangan. Menegaskan bahwa penguatan ketahanan siber hanya dapat tercapai melalui koordinasi lintas-aktor, sehingga tidak dapat bergantung pada negara semata. Oleh karena itu, berbeda dengan pertahanan fisik yang bersifat hierarkis-militeristik, tata kelola ruang siber harus ditempatkan dalam kerangka ekosistem hukum kolaboratif yang melibatkan negara, swasta, dan masyarakat.[53]

D. Penutup

Berdasarkan hasil analisis yang telah dipaparkan, dapat disimpulkan bahwa ancaman siber telah menjadi bentuk ancaman strategis yang tidak lagi dapat dianggap sebelah mata dan menempatkan Indonesia dalam kondisi krisis digital. Ketidakterpaduan kewenangan antara BSSN, TNI, dan Polri, ditambah dengan lemahnya kerangka regulasi teknis, menjadi kendala utama dalam membangun sistem pertahanan siber yang terorganisir dan responsif. Ketiga lembaga tersebut sejatinya

51 Di kutip dari Landasan Etika dan Regulasi AI Berbasis Hukum Transformatif (Bagian II-Habis), kompas.

52 Blassyus Bevry Sinaga, "Pengaturan Teknologi *Blockchain* sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan di Era *Society* 5." *Padjadjaran Law Review*, 12, no. 1 (2024), https://doi.org/10.56895/plr.v12i1.1651.

53 Gabriela Ahmad Assalemi, Haider Al Khateeb, Gregory Epiphaniou, Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Revie w, Smart Cities, 3 (2020), doi: 10.3390/smartcities3030046.

memiliki mandat yang berbeda, tetapi saling melengkapi, sehingga ketidaktegasan dalam pembagian peran justru menimbulkan potensi konflik kewenangan. Penanganan isu siber nasional ke depan memerlukan landasan hukum yang jelas dan mekanisme kelembagaan yang terkoordinasi secara baik. Oleh sebab itu, diperlukan regulasi pelaksana yang mampu menjabarkan batas tanggung jawab, domain operasional, dan mekanisme kerja sama antar lembaga secara detail dan aplikatif.

Saran dari penelitian ini adalah pentingnya pemerintah segera merumuskan suatu sistem hukum yang komprehensif berbasis ius constituendum, guna mendefinisikan batas fungsi, koordinasi teknis, dan sistem respons cepat terhadap ancaman siber. BSSN perlu diperkuat tidak hanya secara kelembagaan, tetapi juga dalam hal kompetensi teknis dan otoritas regulatif, agar mampu menjadi pusat kendali keamanan digital nasional. TNI, sebagai institusi pertahanan, membutuhkan kejelasan hukum terkait peran barunya dalam menghadapi ancaman siber lintas negara, sedangkan Polri perlu diberikan legitimasi penuh untuk menjalankan tugas preventif dan represif terhadap kejahatan digital domestik. Ketiganya harus diarahkan dalam satu sistem kerja yang saling melengkapi, dengan dukungan sumber daya manusia yang profesional dan berkelanjutan. Dengan adanya kejelasan struktur hukum, sinergi lintas sektor, dan pembagian tugas yang proporsional, maka Indonesia akan memiliki sistem keamanan siber yang tangguh, adaptif, dan mampu menjawab tantangan era digital secara efektif.

DAFTAR PUSTAKA

Buku

Asshiddiqie, Jimly, "Perihal Undang-Undang, Depok, Rajawali Press, 2011.

Digdo Ismoyo, Jarot, Apriyanto, Titik Harryato, dan Loso Judijanto. *Teori Negara Hukum Modern*. Jambi: Sonpedia Publishing Indonesia, 2025.

Jalaludin Rifa'i, Iman, Ady Purwoto, Marina Ramadhani, Muksalmina, Muhammad Taufik Rusydi, Nasruddin Khalil Harahap, Ibnu Mardiyanto, dkk. *Metodologi Penelitian Hukum*. Serang: Sada Kurnia Pustaka, 2023.

Laritma, Selfianus, dan Ahmad Rosidi. *Teori-Teori Negara Hukum (Perspektif Kewenangan Mahkamah Agung dalam Melakukan Pengujian Peraturan Perundang-Undangan di Bawah Undang-Undang)*. Jakarta: Kencana, 2024.

Marzuki, Peter Mahmud. Penelitian Hukum: Edisi Revisi. Jakarta: Prenada Media, 2017.

Qurbani, Indah Dwi. "Makna Hukum Dan Kekuasaan: Studi Terhadap Pembentukan Undang-Undang Di Indonesia." In Dinamika Hukum. Malang: Inteligensia Media, 2021.

Soekanto, Soerjono, Faktor-faktor yang Mempengaruhi Penegakan Hukum, Jakarta: Raja Grafindo Persada, 2016.

Soerjono Soekanto, "Pengantar Penelitian Hukum, Jakarta: UI Press, 1968.

Makalah/Artikel/Prosiding/Hasil Penelitian

Ade Irawan, Wildan Hamzah Nur Fadholi, Zahwa Erikamaretha, dan Fried Sinlae. "Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT." *JOURNAL ZETROEM* 6, no. 1 (3 April 2024): 114–19. https://doi.org/10.36526/ztr.v6i1.3376.

Ahmadi-Assalemi, Gabriela, Haider Al-Khateeb, Gregory Epiphaniou, dan Carsten Maple. "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review." *Smart Cities* 3, no. 3 (13 Agustus 2020): 894–927. https://doi.org/10.3390/smartcities3030046.

Anggara Pratama, Apryan, dan Muhammad Ruhly Kesuma Dinata. "Hacker Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data." *Jurnal Hukum Magnum Opus* 6, no. 1 (27 Februari 2023): 14–26. https://doi.org/10.30996/jhmo.v6i1.8293.

Anugrah, Anugrah, dan Rahmat Rahmat. "Pendidikan Karakter dalam Perspektif Kurikulum Pendidikan Pancasila dan Kewarganegaraan (PPKn)." *Jurnal Pendidikan dan Pembelajaran Indonesia (JPPI)* 4, no. 1 (9 Juni 2024): 22–34. https://doi.org/10.53299/jppi.v4i1.403.

Arafat, Muhammad dan Alexander Tito Enggar Wirasto. "Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia." *Equality : Journal of Law and Justice* 1, no. 2 (30 November 2024): 220–41. https://doi.org/10.69836/equality-jlj.v1i2.170.

Astuti, Yunni Widhi. "Peran Masyarakat Dalam Pembentukan Aturan Hukum The Role of Society in Forming the Rule of Law." *Ethics and Law Journal: Business and Notary* 1, no. 3 (28 Desember 2023): 262–74. https://doi.org/10.61292/ELJBN.77.

Balafif, Sabri. "Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework." *Jurnal Informatika: Jurnal Pengembangan IT* 8, no. 3 (10 November 2023): 291–301. https://doi.org/10.30591/jpit.v8i3.5662.

Benuf, Kornelius, dan Muhamad Azhar. "Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (1 April 2020): 20–33. https://doi.org/10.14710/gk.2020.7504.

Budiman, Ahmad. "OPTIMALISASI PERAN BADAN SIBER DAN SANDI NASIONAL." *Majalah Info Singkat Pemerintahan Dalam Negeri* 9, no. 12 (Juni 2017): 17–20.

Chandra, Jansen, Vincent Tanaka, dan Ricky Banke. "Peran Interpol dalam Menangani dan Menanggulangi Kejahatan Siber di Indonesia." *PESHUM: Jurnal Pendidikan,Sosial dan Humaniora* 4, no. 3 (17 April 2025): 4710–19. https://doi.org/10.56799/peshum.v4i3.9028.

Darmawan, Arief Bakhtiar, Kholifatus Saadah, dan I Putu Arya Aditia Utama. "Kedaulatan Negara dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook dan Google." *Jurnal Hubungan Internasional* 16, no. 1 (13 Juli 2023): 211–28. https://doi.org/10.20473/jhi.v16i1.38971.

Dinanda Diadeska Diara. "Strategi Keamanan Siber Korea Selatan." *Jurnal Indonesia Sosial Sains* 1, no. 4 (21 November 2020): 292–305. https://doi.org/10.36418/jiss.v1i4.44.

Dupont, Benoît, dan Chad Whelan. "Enhancing Relationships between Criminology and Cybersecurity." *Journal of Criminology* 54, no. 1 (Maret 2021): 76–92. https://doi.org/10.1177/00048658211003925.

Febriansyah, Ricky, dan Ana Husnayanti. "Keamanan Sistem Informasi Pemilu Melalui Computer Security Incident Response Team (Csirt) Pemilu Serentak 2024." *JIPOSSTER: Jurnal Ilmu Politik dan Studi Sosial Terapan* 3, no. 4 (t.t.): 65–82.

Gandhi, Jennifer, Ben Noble, dan Milan Svolik. "Legislatures and Legislative Politics Without Democracy." *Comparative Political Studies* 53, no. 9 (Agustus 2020): 1359–79. https://doi.org/10.1177/0010414020919930.

Gabriela Ahmad Assalemi, Haider Al Khateeb, Gregory Epiphaniou, Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Revie w, Smart Cities, 3 (2020), doi: 10.3390/smartcities3030046.

Habibah, Siska, Najwa Aulia Widyaningrum, Anisa Mutiara Rizky, dan Fathan Akbar Hernando. "IMPLEMENTASI KONSEP CHECK AND BALANCE PETER L. STRAUSS DALAM SISTEM KELEMBAGAAN INDONESIA." *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 1 (25 Januari 2025): 359–67. https://doi.org/10.59141/cerdika.v5i1.2431.

Haryadi, Eko Haryadi, Diah Wijayanti, Eka Chadra Ramdhani, dan Indria Widyastuti. "Identifikasi Ancaman Keamanan Siber Dari Penyalahgunaan Sumber Daya Tik: Studi Kasus Perusahaan Polymer." *Technologia : Jurnal Ilmiah* 15, no. 4 (8 Oktober 2024): 886–96. https://doi.org/10.31602/tji.v15i4.16429.

---

67 Cedric Thompson, "Global Reporting Initiative (GRI): Purpose, Standards, and Importance," Investopedia, 2023, https://www.investopedia.com/global-reporting-initiative-7483127.

68 Vinay Kandpal dkk., "Corporate Social Responsibility (C.S.R.) and E.S.G. Reporting: Redefining Business in the Twenty-First Century," dalam *Sustainable Energy Transition*, oleh Vinay Kandpal dkk., Circular Economy and Sustainability (Cham: Springer Nature Switzerland, 2024), 239–72, https://doi.org/10.1007/978-3-031-52943-6_8.

Haryanto, Agus, dan Satya Muhammad Sutra. "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020." *Global Political Studies Journal* 7, no. 1 (30 April 2023): 56–69. https://doi.org/10.34010/gpsjournal.v7i1.8141.

I Nengah Sudiarta. "Pengaturan Hak Asasi Manusia Dalam Sistem Hukum Nasional." *IJOLARES : Indonesian Journal of Law Research* 2, no. 1 (30 Maret 2024): 25–31. https://doi.org/10.60153/ijolares.v2i1.44.

Juaningsih, Imas Novita, Rayhan Naufaldi Hidayat, Kiki Nur Aisyah, dan Dzakwan Nurirfan Rusli. "Rekonsepsi Lembaga Pengawas terkait Perlindungan Data Pribadi oleh Korporasi sebagai Penegakan Hak Privasi berdasarkan Konstitusi." *SALAM: Jurnal Sosial dan Budaya Syar-i* 8, no. 2 (5 Maret 2021): 469–86. https://doi.org/10.15408/sjsbs.v8i2.19904.

La Adu, Arifin, Rudy Hartanto, dan Silmi Fauziati. "HAMBATAN-HAMBATAN DALAM IMPLEMETASI LAYANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) PADA PEMERINTAH DAERAH." *JIKO (Jurnal Informatika dan Komputer)* 5, no. 3 (15 Desember 2022): 215–23. https://doi.org/10.33387/jiko.v5i3.5344.

Li, Yun, Muhammad Naeem Shahid, Muhammad Umar Islam, dan Fatema Deme. "The Role of Green Technological Innovation, Fintech, and Financial Development in Environmental Sustainability: A Study on Selected Asian Countries." *Journal of Economics, Finance and Accounting Studies* 6, no. 3 (11 Mei 2024): 67–76. https://doi.org/10.32996/jefas.2024.6.3.4.

Madinah Mokobombang, Zulfikri Darwis, dan Sabil Mokodenseho. "Pemberantasan Tindak Pidana Cyber di Provinsi Jawa Barat: Peran Hukum dan Tantangan dalam Penegakan Hukum Terhadap Kejahatan Digital." *Jurnal Hukum dan HAM Wara Sains* 2, no. 06 (28 Juni 2023): 517–25. https://doi.org/10.58812/jhhws.v2i6.447.

McGlave, Claire C, Sayeh S Nikpay, Carrie Henning-Smith, Katie Rydberg, dan Hannah T Neprash. "Characteristics of Short-Term Acute Care Hospitals That Experienced a Ransomware Attack from 2016 to 2021." *Health Affairs Scholar* 1, no. 3 (4 September 2023): 1–5. https://doi.org/10.1093/haschl/qxad037.

Nawawi, Hafiz Pratama S, Carrudin, dan Dadang Yusup. "ANALISIS PENEMUAN BARANG BUKTI DIGITAL MELALUI REKAMAN SUARA MENGGUNAKAN PRAAT DENGAN METODE AUDIO FORENSIK." *CyberSecurity dan Forensik Digital* 4, no. 2 (19 April 2024): 96–103. https://doi.org/10.14421/csecurity.2021.4.2.2638.

Okori, Washington, dan Sarah Buteraba. "Cyber Security Exploits and Management in Telecommunication Companies: The Case of Uganda." *Journal of Computer Science and Technology Studies* 6, no. 4 (5 Oktober 2024): 67–76. https://doi.org/10.32996/jcsts.2024.6.4.10.

Polevaya, Elena, dan Irina Shustova. "The Impact of Digitalization on Organizational Management Structures." Disunting oleh V. Pukhkal dan S. Uvarova. *E3S Web of Conferences* 458, no. 04007 (2023): 1–8. https://doi.org/10.1051/e3sconf/202345804007.

Ramayanti, Herni, dan Arief Fahmi Lubis. "Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional." *Jurnal Hukum dan HAM Wara Sains* 2, no. 9 (29 September 2023): 904–12. https://doi.org/10.58812/jhhws.v2i09.672.

Refnaldi Kurniawan Saputra, Gyna Rahmi Fajri, Sya'banu Ahmad, Ewa Haris Sembiring, dan Mhd Arief Hasan. "KEAMANAN DATA PADA PENGARSIPAN SURAT MENGGUNAKAN METODE KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN SHIFT CIPHER." *ZONAsi: Jurnal Sistem Informasi* 2, no. 1 (6 Maret 2021): 61–72. https://doi.org/10.31849/zn.v2i1.6220.

Robles-Carrillo, M., dan P. García-Teodoro. "Ransomware: An Interdisciplinary Technical and Legal Approach." Disunting oleh Helena Rifà-Pous. *Security and Communication Networks* 2022 (1 Agustus 2022): 1–17. https://doi.org/10.1155/2022/2806605.

Rosy, Afifah Fidina. "Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber: Indonesia's International Cooperation: Strengthening National Security in the Field of Cyber Security." *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan* 1, no. 2 (22 Juli 2020): 118–29. https://doi.org/10.54144/govsci.v1i2.12.

Shiddique, Muhammad Rafi, dan Mansur Juned. "Human Capital Development for Cybersecurity: Examining BSSN's

Contributions in the Indonesia-Australia Cyber Policy Dialogue (2018-2020)." *Journal of Social and Political Sciences* 6, no. 4 (30 Desember 2023): 215–24. https://doi.org/10.31014/aior.1991.06.04.457.

Simada, Arthur, Syafruddin Kalo, Mohammad Ekaputra, dan Jelly Leviza. "Penentuan Locus Delictie dalam Tindak Pidana Cyber Crime (Merusak dan Mengganggu Sistem Elektronik dan Komunikasi Milik Orang Lain)." *Locus Journal of Academic Literature Review* 3, no. 4 (29 April 2024): 349–61. https://doi.org/10.56128/ljoalr.v3i4.314.

Situmorang, Christian Immanuel, Rafli Akmal Athallah, Frans Samuel Junero Butar Butar, dan Irwan Triadi. "Pentingnya Hukum yang Tegas dalam Mempertahankan Hak Asasi Manusia: Perspektif Konstitusi: (The Importance of Strict Law in Defending Human Rights: A Constitutional Perspective)." *Journal Customary Law* 1, no. 2 (8 Mei 2024): 1–13. https://doi.org/10.47134/jcl.v1i2.2427.

Sukmawan, Denny Indra, dan David Putra Setyawan. "Hacker, Fear, and Harm: Data Breaches and National Security." *Jurnal Global & Strategis* 17, no. 1 (30 Mei 2023): 153–82. https://doi.org/10.20473/jgs.17.1.2023.153-182.

Tiara Saskia Maharani. "Law Enforcement Regarding Human Rights According to Positive Law in Indonesia." *Journal of Strafvordering Indonesian* 1, no. 1 (12 Maret 2024): 1–5. https://doi.org/10.62872/n1f51e68.

Waskita, Allisa Salsabilla, dan Hasan Sidik. "Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019." *Padjadjaran Journal of International Relations* 5, no. 2 (6 Agustus 2023): 142–64. https://doi.org/10.24198/padjir.v5i2.41337.

Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review, Smart Cities, 3 (2020), doi: 10.3390/smartcities3030046.

Internet

Wachid Anshory, Wahyu. "Peran Baru TNI Perangi Ancaman Siber, Apa Bedanya dengan Komdigi dan BSSN?" *kompas.com*, 26 Maret 2025. https://www.kompas.com/jawa-barat/read/2025/03/26/173000488/peran-baru-tni-perangi-ancaman-siber-apa-bedanya-dengan-komdigi-dan.

Randra, Typama. "Heboh PeduliLindungi Berubah Jadi Laman Judol." *news.detik.com*, 22 Mei 2025. https://news.detik.com/berita/d-7925829/heboh-pedulilindungi-berubah-jadi-laman-judol.

Gabriella, Michelle. "Pusat Data Nasional Jebol hingga Permintaan Tebusan Rp 131 Miliar, Ini Kilas Balik Kasusnya." *Tempo.co*, 24 Juni 2024. https://www.tempo.co/hukum/pusat-data-nasional-jebol-hingga-permintaan-tebusan-rp-131-miliar-ini-kilas-balik-kasusnya-45802.

Peraturan Perundang-Undangan

Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.

Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 2 Tahun 2002 tentang Kepolisian Republik Indonesia.

Undang-Undang No. 34 Tahun 2004 tentang Tentara Nasional Indonesia.

Undang-Undang Nomor 3 Tahun 2025 perubahan atas Undang-Undang No. 34 Tahun 2004 tentang Tentara Nasional Indonesia.