



Jurnal Kompilasi Hukum

Volume 10, No. 2, December 2025, E-ISSN 2598-6414, P-ISSN 2502-5333

Publisher Magister of Law, Faculty of Law Mataram University,

open access at : <http://jkh.unram.ac.id>

REVISI UNDANG-UNDANG TNI DAN HAK DIGITAL WARGA NEGARA: ANTARA KEAMANAN NASIONAL DAN TANTANGAN DEMOKRASI DIGITAL

REVISION OF THE INDONESIAN ARMED FORCES LAW AND CITIZENS' DIGITAL RIGHTS: BETWEEN NATIONAL SECURITY AND THE CHALLENGES OF DIGITAL DEMOCRACY

Dimas Kurnia Iqram

Universitas Bengkulu

Email: dimasiqram06@gmail.com

Ilham Agusyanda

Universitas Bengkulu

Email: ilhamagusyanda06@gmail.com

Dody Heryanto Sitorus

Universitas Bengkulu

Email: dodisitorus37@gmail.com

Abstrak

Kemajuan teknologi informasi telah membawa transformasi signifikan dalam berbagai aspek kehidupan masyarakat, termasuk dalam hal perlindungan hak asasi manusia di era digital. Disahkannya Revisi Undang-Undang TNI tahun 2025 memperluas peran militer ke sektor keamanan siber, yang memunculkan kekhawatiran mengenai potensi pelanggaran hak-hak digital warga negara, seperti hak privasi, kebebasan berpendapat, dan akses terhadap informasi. Penelitian ini bertujuan untuk mengkaji dampak yang mungkin timbul dari perluasan fungsi TNI di ranah siber terhadap hak digital warga negara berdasarkan perspektif demokrasi digital dan prinsip-prinsip konstitusi. Metode penelitian yang diterapkan menggunakan pendekatan normatif melalui analisis hukum, studi pustaka, serta evaluasi kritis atas praktik ketatanegaraan pasca perubahan UU TNI. Studi ini menemukan bahwa revisi Undang-Undang TNI yang memperluas keterlibatan militer dalam ranah keamanan siber berpotensi memperkuat kapasitas negara dalam menghadapi ancaman digital, namun sekaligus menimbulkan risiko terhadap perlindungan hak digital warga negara, terutama terkait privasi, kebebasan berekspresi, dan perlindungan data pribadi. Dari perspektif demokrasi digital, penguatan keamanan nasional perlu diimbangi dengan mekanisme kontrol sipil yang efektif, transparansi regulasi, serta kepastian batas kewenangan militer di ruang siber agar tidak terjadi tumpang tindih peran dengan otoritas sipil. Penelitian ini merekomendasikan penyusunan aturan turunan yang lebih jelas mengenai ruang lingkup tugas TNI di bidang siber, penguatan peran lembaga pengawas independen, serta integrasi prinsip hak asasi manusia ke dalam kebijakan keamanan digital guna memastikan bahwa upaya menjaga keamanan nasional tetap sejalan dengan nilai demokrasi dan perlindungan hak warga negara.

Kata kunci: *hak, digital, demokrasi, TNI*

Abstract

Advances in information technology have brought significant transformations to various aspects of society, including the protection of human rights in the digital era. The enactment of the 2025 Revised Indonesian National Armed Forces Law expands the military's role into cybersecurity,



Copyright (c) 2025 by Author(s). This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License. DOI: <https://doi.org/10.29303/jkh.v10i2.279>

raising concerns about potential violations of citizens' digital rights, such as the right to privacy, freedom of expression, and access to information. This study aims to examine the potential impact of the TNI's expanded cyberspace role on citizens' digital rights, based on a digital democracy perspective and constitutional principles. The research method employed is a normative approach through legal analysis, literature review, and a critical evaluation of state practices following the amendment to the TNI Law. This study finds that the revised TNI Law, which expands military involvement in cybersecurity, has the potential to strengthen the state's capacity to address digital threats, but also poses risks to the protection of citizens' digital rights, particularly those related to privacy, freedom of expression, and personal data protection. From a digital democracy perspective, strengthening national security needs to be balanced with effective civilian oversight mechanisms, regulatory transparency, and certainty about the limits of military authority in cyberspace to prevent overlapping roles with civilian authorities. This study recommends the development of clearer derivative regulations regarding the scope of the TNI's duties in the cyber sector, strengthening the role of independent oversight bodies, and integrating human rights principles into digital security policies to ensure that efforts to maintain national security remain in line with democratic values and the protection of citizens' rights.

Keywords: *rights, digital, democracy, TNI*

PENDAHULUAN

Dinamika dan perubahan zaman digital terhadap kemajuan teknologi telah berkontribusi secara faktual dalam berbagai sisi kehidupan manusia. Kemajuan teknologi informasi yang serba digital ini membawa dampak revolusioner (*Digital Revolution Era*), yang disebabkan karena menciptakan sistem yang mempermudah kehidupan khalayak banyak¹. Salah satu aspek yang mengalami perkembangan pesat di era digital saat ini adalah pemanfaatan internet. Saat ini pemanfaatan internet tidak hanya diperuntukkan sebagai media hiburan, namun internet juga dimanfaatkan pada kegiatan lainnya seperti sekolah, bekerja, pelayanan kesehatan, dan bahkan dalam bidang politik dan pemerintahan. Menurut data yang dilansir dari laman Teknologi.id, pada tahun 2025 APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) mencatat jumlah pengguna internet di Indonesia mencapai 229 juta jiwa.² Jika dibandingkan dengan data lima tahun sebelumnya pada 2020 yang hanya sebesar 175,4 juta pengguna, *Status Quo* saat ini menunjukkan adanya peningkatan yang sangat signifikan dalam penggunaan internet di Indonesia.³

Perkembangan zaman menuju era digitalisasi telah melahirkan transformasi yang fundamental dalam berbagai sektor kehidupan, termasuk dalam ranah konstruksi hukum saat ini. Kemajuan teknologi informasi dan komunikasi, khususnya di era digital saat ini, telah mendorong terjadinya evolusi substansial dalam sistem hukum di Indonesia, baik dari segi substansi hukum, prosedur penegakan hukum, maupun kelembagaan penegak hukum itu sendiri.⁴

1 Reda Manthovani, *Penyadapan vs. Privasi*, PT Bhuana Ilmu Populer, Jakarta, 2013, hal 35

2 Shabrina, S. (2025, Agustus 07). "Jumlah Pengguna Internet Indonesia Tembus 229 Juta pada 2025," *Teknologi.id*, <https://teknologi.id/teknologi/apjii-rilis-data-terbaru-2025-pengguna-internet-di-indonesia-capai-229-juta-jiwa>, diakses 17 Agustus 2025.

3 Puspitasari, K. (2022, Agustus 13). "Perlindungan hak asasi digital. Sekretariat Kabinet Republik Indonesia". <https://setkab.go.id/perlindungan-hak-asasi-digital/>, diakses 10 April 2025

4 Hukum UMA. (2024, September 6). Evolusi hukum pidana di era digital: Tantangan dan peluang. <https://hukum.uma.ac.id/2024/09/06/evolusi-hukum-pidana-di-era-digital-tantangan-dan-peluang/>, diakses 10 April 2025

Selain itu juga dalam perkembangannya teknologi digital saat ini juga telah membawa dinamika baru dalam perlindungan hak asasi manusia, terutama yang berkaitan dengan hak-hak digital. Perkembangan teknologi informasi memungkinkan dilakukannya pengumpulan, pengolahan, dan analisis data pribadi dalam skala masif melalui berbagai platform digital. Praktik ini, apabila tidak diimbangi dengan regulasi yang ketat dan mekanisme pengawasan yang memadai, berpotensi mengancam hak atas privasi individu, yang merupakan bagian integral dari Hak Asasi Manusia (HAM) sebagaimana diatur dalam berbagai instrumen internasional maupun peraturan perundang-undangan nasional. Teknologi digital juga memberikan pengaruh signifikan terhadap pemenuhan hak-hak sipil dan politik, antara lain hak atas kebebasan berekspresi dan hak atas akses terhadap informasi. Di satu sisi, teknologi digital membuka ruang partisipasi publik yang lebih luas. Namun di sisi lain, teknologi ini juga dapat dimanfaatkan untuk hal-hal yang bersifat eksese, yang salah satunya dilakukan dengan membatasi kebebasan berekspresi, seperti penyensoran konten secara sewenang-wenang maupun melalui penyalahgunaan sistem algoritma yang dapat menimbulkan bentuk baru dari diskriminasi digital (*algorithmic discrimination*). Di samping itu, ancaman terhadap keamanan siber (*cybersecurity threats*) dan problematika seputar anonimitas dalam ruang digital turut menimbulkan kompleksitas tersendiri dalam penegakan hak-hak digital.⁵

Hak digital merupakan bagian yang tidak terpisahkan dari rezim hak asasi manusia kontemporer, khususnya dalam konteks masyarakat yang semakin terdigitalisasi. Istilah ini mencakup seperangkat hak yang dimiliki individu untuk mengakses, memanfaatkan, memproduksi, dan mendistribusikan informasi atau karya digital, serta hak atas akses terhadap perangkat teknologi dan jaringan komunikasi, namun tidak terbatas pada internet. Hak digital tidak hanya menjadi sarana bagi partisipasi aktif dalam kehidupan sosial, ekonomi, dan politik, tetapi juga merupakan manifestasi konkret dari prinsip-prinsip kebebasan berekspresi, hak atas informasi, serta perlindungan atas integritas dan otonomi pribadi di ruang digital. Dalam sistem hukum nasional Indonesia, jaminan terhadap hak digital secara eksplisit dapat ditemukan dalam ketentuan Pasal 28F dan 28E ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Kemudian pasal tersebut diejawantahkan melalui aturan turunannya yang diakomodir melalui Undang-Undang Nomor 9 Tahun 1998 tentang Kemerdekaan Menyampaikan Pendapat di Muka Umum. Pada Pasal 1 Ayat (1) yang secara eksplisit dijelaskan melalui frasanya bahwa “*kemerdekaan menyampaikan pikiran dengan lisan, tulisan dan sebagainya secara bebas dan bertanggungjawab sesuai dengan ketentuan perundangan yang berlaku.*”⁶ Jaminan konstitusional tersebut memperoleh penguatan normatif melalui peraturan perundang-undangan sektoral, yang antara lain mensyaratkan adanya persetujuan eksplisit dari pemilik data dalam hal penggunaan informasi pribadi melalui media elektronik.⁷

Indonesia memiliki lembaga yang secara khusus menangani urusan siber dan perlindungan digital. Lembaga tersebut diatur melalui Peraturan Presiden Republik In-

5 Ginanjar, D., Firdausyi, M. F., Suswandy, S., & Andini, N. T. (2022). *Perlindungan HAM dalam era digital: Tantangan dan solusi hukum*. Journal on Education, 4(4), hal. 2084

6 Nasution, L. (2020). *Hak kebebasan berpendapat dan berekspresi dalam ruang publik di era digital*. Adalah, 4(3), hal. 38

7 Puspitasari, K., *op. cit.*

donesia Nomor 28 Tahun Tentang Badan Siber Dan Sandi Negara. Badan Siber dan Sandi Negara (BSSN) sejatinya tidak secara mutlak merupakan lembaga baru, melainkan merupakan hasil transformasi institusional melalui proses integrasi dan penggabungan dari dua entitas yang sebelumnya telah menjalankan fungsi serupa dalam bidang keamanan informasi dan persandian, yakni Lembaga Sandi Negara (Lemsaneg) dan Direktorat Keamanan Informasi pada Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika (Kemenkominfo).⁸

Pada tanggal 20 maret 2025, DPR RI melalui ketua DPR RI Puan Maharani meresmikan Revisi Undang-Undang Tentang Tentara Nasional Indonesia menjadi undang-undang. Peresmian ini menuai kritik dan respon masyarakat dari berbagai kalangan. Revisi Undang-undang yang telah disahkan tersebut menimbulkan kekhawatiran yang serius khususnya yang berkaitan terhadap perluasan kewenangan militer di ranah siber, yang mana didalam Pasal 47 Ayat (1) Undang-Undang Nomor 3 Tahun 2025 Tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 Tentang Tentara Nasional Indonesia menjelaskan melalui frasanya bahwa “Prajurit dapat menduduki jabatan yang salah satunya menangani urusan Siber dan/atau Sandi Negara”.⁹ Penambahan tugas TNI dalam Operasi Militer Selain Perang (OMSP), khususnya dalam menanggulangi ancaman pertahanan siber, secara potensial menciptakan tumpang tindih kewenangan dengan lembaga sipil seperti Kementerian Komunikasi dan Digital (komdigi) serta Badan Siber dan Sandi Negara, hal ini dapat mengaburkan batas antara fungsi militer dan sipil dalam pengelolaan ruang digital.¹⁰ Hal yang dikhawatirkan lagi adalah perluasan kewenangan TNI ini dapat mengancam kebebasan hak digital warga negara yang merupakan bagian integral dari hak asasi manusia yang dijamin oleh UUD NRI 1945.

Mengutip dari Tempo.co bahwa narasi militerisasi ruang siber yang terkandung dalam revisi UU TNI sangat berbahaya bagi penghormatan terhadap hak-hak digital masyarakat Indonesia. Perluasan kewenangan OMSP untuk mengatasi dimensi virtual dan kognitif dari perang siber dapat diinterpretasikan secara luas sehingga sangat rentan disalahgunakan. Proses pembahasan revisi UU TNI juga menuai kritik karena dinilai tidak memenuhi transparan dan minim partisipasi publik (*Meaningful Participation*). Pengamat hukum Universitas Mulawarman, Herdiansyah Hamzah, menyampaikan bahwa revisi tersebut berpotensi membuka kembali dominasi militer di ruang sipil dan politik, serta mengancam demokrasi. Ketidakjelasan batasan kewenangan antara TNI dan lembaga sipil dalam menangani ancaman siber dapat menimbulkan konflik kepentingan dan memperlemah akuntabilitas institusi negara.¹¹

Meskipun secara normatif dapat dibenarkan dalam konteks perlindungan negara, pelibatan militer dalam ranah siber menimbulkan kekhawatiran akan terjadinya *Overreach* atau perluasan kekuasaan tanpa pengawasan yang memadai. Ketidakjelasan pem-

8 Badan Siber dan Sandi Negara. (n.d.). Tentang BSSN, <https://www.bssn.go.id/tentang-bssn/> , diakses pada 11 April 2025

9 Undang-Undang Nomor 3 Tahun 2025 Tentang Perubahan Atas Undang-Undang Nomor 34 Tahun 2004 Tentang Tentara Nasional

10 Berita Borneo. (n.d.). “Seusai UU TNI disahkan: Bagaimana kewenangan TNI di dunia siber?”, <https://beritaborneo.com/main/seusai-uu-tni-disahkan-bagaimana-kewenangan-tni-di-dunia-siber/>, diakses 15 April 2025

11 Goodkind. (n.d.). RUU TNI disahkan: Pengamat - Ruang digital warga akan dikontrol kekuasaan. <https://goodkind.id/tulisan/ruu-tni-disahkan-pengamat-ruang-digital-warga-akan-dikontrol-oleh-kekuasaan/>, diakses 22 April 2025

bagian kewenangan antara militer dan badan sipil seperti BSSN maupun Kementerian Komunikasi dan Informatika (Kemenkominfo) justru berpotensi menimbulkan konflik yurisdiksi dan mengaburkan akuntabilitas publik.¹² Keterlibatan militer dalam urusan sipil bukan hal baru dalam sejarah politik Indonesia. Masa Orde Baru menjadi preseden yang sarat akan praktik militeristik dalam mengontrol ruang publik, membatasi kebebasan sipil, dan melakukan represi terhadap oposisi politik. Kini, kekhawatiran yang sama kembali mengemuka, namun dalam bentuk yang lebih canggih dan tersembunyi melalui alasan keamanan siber.¹³ TNI berpotensi melakukan pengawasan siber terhadap aktivitas warga negara tanpa mekanisme akuntabilitas publik yang ketat, sehingga membuka ruang terjadinya pelanggaran hak asasi manusia. Represi yang dahulu dilakukan secara fisik dan terbuka, kini dapat berganti rupa menjadi pengawasan algoritmik, sensor digital, hingga pembungkaman ruang diskusi daring melalui justifikasi ancaman keamanan nasional. Tanpa kejelasan pembatasan kewenangan militer, kekuasaan digital dapat digunakan untuk mengontrol opini publik dan meredam suara-suara kritis terhadap pemerintah.

Karya tulis ilmiah ini berjudul “Implikasi Revisi Undang-Undang Tentara Nasional Indonesia Terhadap Hak Digital Warga Negara: Perspektif Demokrasi” dan bertujuan untuk membedah secara komprehensif ancaman potensial yang dapat mereduksi hak-hak warga negara dalam ranah digital, sekaligus menelaah bagaimana negara dapat menjamin perlindungan terhadap hak-hak tersebut di era 5.0. Identifikasi masalah yang diangkat berfokus pada dua aspek utama. **Pertama**, bagaimana tata kelola keamanan siber yang ideal dapat diwujudkan dalam suatu negara demokrasi, sehingga mampu menjaga keseimbangan antara kebutuhan keamanan nasional dan perlindungan hak asasi digital warga negara. **Kedua**, bagaimana dampak potensial dari perluasan fungsi Tentara Nasional Indonesia (TNI) dalam bidang keamanan siber dapat memengaruhi hak digital warga negara Indonesia, khususnya dalam konteks kebebasan berekspresi, privasi, dan partisipasi publik di ruang digital.

Tujuan penelitian ini adalah untuk mengetahui dan menganalisis tata kelola keamanan siber yang sesuai dengan prinsip demokrasi, yakni tata kelola yang transparan, akuntabel, serta berorientasi pada perlindungan hak asasi manusia. Selain itu, penelitian ini juga bertujuan untuk mengkaji secara kritis dampak dari perluasan fungsi TNI dalam bidang keamanan siber terhadap hak digital warga negara, dengan menimbang potensi terjadinya militerisasi ruang digital yang dapat mengancam kebebasan sipil. Dengan demikian, penelitian ini diharapkan mampu memberikan kontribusi akademik dalam merumuskan model tata kelola keamanan siber yang demokratis sekaligus memberikan rekomendasi kebijakan yang menjamin perlindungan hak digital warga negara Indonesia.

Penelitian ini merupakan penelitian hukum (*legal research*) yang secara khusus diterapkan dalam bidang ilmu hukum. Menurut Peter Mahmud Marzuki, penelitian ini

12 Kompas. (2025, April 2). Sipil dan Militer dalam Penjagaan Ruang Siber. <https://nasional.kompas.com/read/2025/04/02/08061311/sipil-dan-militer-dalam-penjagaan-ruang-siber?page=all>, diakses 29 April 2025

13 Media Indonesia. (2025, Maret 29). *SAFEnet: Revisi UU TNI Berdampak pada Militerisasi Ruang Siber, Hak Digital Publik Akan Terancam*. <https://mediaindonesia.com/politik-dan-hukum/753532/safenet-revisi-uu-tni-berdampak-pada-militerisasi-ruang-siber-hak-digital-publik-akan-terancam>, diakses 29 Maret 2025

melibatkan mengevaluasi aturan hukum dan prinsip-prinsipnya sebagai cara untuk menyelesaikan masalah hukum yang muncul¹⁴. Pendekatan yang digunakan adalah yuridis normatif, yaitu pendekatan yang dikenal pula sebagai penelitian doktrinal (*doctrinal research*), yang bertujuan untuk mengkaji ketentuan hukum yang tertulis (*law as it is written in the book*) maupun putusan hakim melalui proses peradilan (*law as it is decided by the judge through judicial process*).

Pengumpulan data dilakukan dengan metode studi kepustakaan (*library research*), yakni dengan meneliti bahan-bahan yang termasuk dalam kategori data sekunder. Data tersebut meliputi:

1. Bahan hukum primer, yaitu berbagai peraturan perundang-undangan yang bersifat mengikat dan dikeluarkan oleh lembaga yang berwenang, seperti Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia beserta revisinya tahun 2025, serta peraturan lain terkait keamanan siber dan perlindungan hak digital.
2. Bahan hukum sekunder, yakni sumber-sumber yang memberikan penjelasan atau komentar atas bahan hukum primer, seperti buku teks, artikel jurnal hukum, karya ilmiah tentang demokrasi digital dan keamanan siber, serta referensi daring yang relevan.
3. Bahan hukum tersier, yaitu referensi yang membantu menjelaskan bahan hukum primer dan sekunder, antara lain kamus hukum, ensiklopedia, dan indeks pustaka.

Penelitian ini menggabungkan pendekatan konseptual dan pendekatan perundang-undangan untuk menelaah prinsip-prinsip negara hukum, supremasi sipil, serta perlindungan hak-hak digital warga negara dalam konteks perluasan peran militer di ranah siber.

ANALISIS DAN PEMBAHASAN

1. Tata Kelola Keamanan Siber yang Ideal Dalam Negara Demokrasi

- a. Perbandingan Terhadap Kewenangan di Bidang Keamanan Siber Sebelum dan Sesudah RUU TNI Disahkan

Sebelum hadirnya Undang-Undang Nomor 3 Tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, kewenangan di bidang keamanan siber dilaksanakan sepenuhnya oleh unsur sipil berdasarkan rambu-rambu yang pelaksanaannya telah ditetapkan sebagai wujud komitmen strategis dan berkelanjutan dalam membangun sistem keamanan siber nasional yang responsif. Komitmen tersebut dijawab tahnkan melalui Peraturan Presiden Nomor 28 Tahun 2021 Tentang Badan Siber dan Sandi Negara, Yang mana Perpres ini menetapkan BSSN sebagai lembaga pemerintah non-kementerian yang berada di bawah dan bertanggung jawab kepada Presiden melalui menteri yang mengoordinasikan bidang politik, hukum, dan keamanan. BSSN bertugas melaksanakan keamanan siber secara

14 PDM Marzuki, *Penelitian Hukum: Edisi Revisi*, (Prenada Media, 2017), hal 54

efektif dan efisien dengan mengkonsolidasikan semua unsur terkait keamanan siber di Indonesia.¹⁵

Selain itu, Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara ini juga merupakan dasar hukum utama bagi BSSN dalam melaksanakan tugasnya untuk melindungi, menjaga keamanan, dan menjamin kedaulatan ruang siber Indonesia. Selain sebagai instrumen penataan kelembagaan, Perpres ini juga menegaskan peran BSSN dalam mendukung pertumbuhan ekonomi nasional melalui penciptaan stabilitas keamanan digital yang adaptif terhadap dinamika ancaman siber.¹⁶ Untuk memastikan efektivitas organisasi, struktur dan tata kerja BSSN diatur lebih lanjut melalui Peraturan Kepala BSSN Nomor 6 Tahun 2021 yang mengatur secara teknis pembagian tugas, mekanisme koordinasi, serta hierarki kewenangan antar unit kerja di lingkungan BSSN.

BSSN dalam pembentukannya diperuntukan untuk melakukan pemanfaatan, pengembangan, dan konsolidasi seluruh unsur yang berkaitan dengan pengamanan ruang siber Indonesia, dengan tujuan untuk membangun sistem pertahanan digital yang tangguh dan adaptif terhadap dinamika ancaman di era informasi. Dalam pelaksanaannya, BSSN berpedoman pada lima pilar *Global Cybersecurity Index* (GCI), yakni aspek hukum, teknis, organisasi, pengembangan kapasitas, dan kerja sama, yang tidak hanya berfungsi sebagai dasar perumusan kebijakan dan program, tetapi juga sebagai tolak ukur kesiapan dan kapabilitas nasional dalam menghadapi berbagai bentuk serangan siber. BSSN dalam tugasnya membentuk *Government Computer Security Incident Response Team* (Gov-CSIRT) yang menangani insiden siber pada sektor pemerintahan, mengembangkan sistem pelaporan dan penanganan insiden, serta menetapkan standar keamanan dan sertifikasi profesional di bidang keamanan informasi. Dalam menjalankan tugasnya BSSN dilengkapi dengan fungsi koordinasi dan harmonisasi lintas sektor, termasuk penyusunan Strategi Keamanan Siber Nasional dan matriks pengukuran keamanan siber yang berfungsi sebagai instrumen evaluatif terhadap pencapaian dan identifikasi kerentanan di tingkat nasional dan daerah.¹⁷

Disisi lainnya juga, dalam rangka meningkatkan pertahanan negara Indonesia, Badan Siber dan Sandi Negara (BSSN) diberikan kewenangan untuk dapat menjalin kemitraan strategis dengan Tentara Nasional Indonesia (TNI), khususnya dalam bidang pertahanan siber. Ketentuan ini diatur dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber. Kerja sama ini didasarkan pada pembagian domain antara keamanan siber sipil yang menjadi tanggung jawab BSSN, dan pertahanan siber negara yang berada di bawah otoritas TNI.¹⁸ TNI menyelenggarakan pertahanan siber untuk menghadapi ancaman eksternal yang berpotensi mengganggu kedaulatan dan integritas nasional, sementara BSSN fokus

15 SYAFIUL HADI, "Wiranto Akan Resmikan Badan Siber Dan Sandi Negara Bulan Ini," TEMPO, 2017, <https://www.tempo.co/politik/wiranto-akan-resmikan-badan-siber-dan-sandi-negara-bulan-ini-1156991>, diakses 11 April 2025

16 ID-SIRTII. (n.d.). "Badan Siber dan Sandi Negara". <https://idsirtii.or.id/bssn.html>, diakses 10 April 2025

17 Agus Haryanto and 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 (2023), hal 63-66.

18 Nurmaida Delviana, Inisiasi Pembentukan Angkatan Siber Dan Digital Dalam Organisasi Tentara Nasional Indonesia, *Jurnal Syntax Admiration* 5, no. 2, (2024), hal 397.

pada pengelolaan keamanan siber domestik, perlindungan infrastruktur informasi vital, serta koordinasi insiden siber di tingkat nasional. Relasi antara BSSN dan TNI bersifat koordinatif dan saling melengkapi, dengan ruang lingkup tugas yang berbeda namun kerap bersinggungan.

Kolaborasi antara Badan Siber dan Sandi Negara (BSSN) dan Tentara Nasional Indonesia (TNI) dalam bidang keamanan dan pertahanan siber mencakup berbagai aspek strategis, termasuk pertukaran informasi intelijen, pengembangan kapasitas sumber daya manusia, dan penyusunan protokol penanganan insiden siber nasional. Sinergi antara kedua institusi ini menjadi sangat penting mengingat sifat serangan siber yang kerap bersifat lintas batas, kompleks, dan sulit diidentifikasi pelakunya secara jelas (*attribution problem*). Dalam perspektif hukum tata negara, pola kerja sama ini mencerminkan pendekatan *whole-of-government*, di mana BSSN dan TNI secara terpadu menjalankan fungsi pemerintahan dalam bidang yang memiliki irisan antara keamanan dan pertahanan. Hubungan antara keduanya bersifat koordinatif dan fungsional, dengan orientasi pada penciptaan sistem pertahanan dan keamanan siber negara yang terintegrasi dan responsif terhadap dinamika ancaman global¹⁹.

Namun dengan terjadinya perubahan regulasi yang terjadi pada Maret 2025 yakni pada Undang-Undang Tentara Nasional Indonesia khususnya secara pada kewenangan TNI dalam menjalankan tugas-tugas pertahanan di ruang siber, sebagaimana tercantum dalam Pasal 7 ayat (2b) hasil revisi. Pengaturan baru tersebut menegaskan posisi TNI dalam Operasi Militer Selain Perang, khususnya dalam menanggulangi ancaman yang berasal dari dunia digital. Jika sebelumnya keterlibatan TNI dalam isu-isu siber terbatas pada penugasan khusus dari pemerintah dan bersifat pendukung, kini TNI memperoleh mandat legal untuk secara aktif menghadapi serangan terhadap sistem pertahanan nasional, peretasan data strategis, sabotase infrastruktur digital, hingga serangan terhadap instalasi vital seperti jaringan listrik, sistem transportasi, dan telekomunikasi nasional. Selain itu, melalui Pasal 47 ayat (1), revisi tersebut juga memperkenankan prajurit aktif TNI untuk menduduki jabatan sipil strategis di instansi seperti BSSN dan Komdigi, yang secara normatif berpotensi menimbulkan kaburnya batas antara ranah sipil dan militer.²⁰

Pada Pasal 47 ayat (2) tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, TNI diberikan kewenangan untuk dapat menduduki jabatan di lembaga siber dan/atau sandi negara tanpa harus mengundurkan diri atau pensiun dini dari dinas aktif keprajuritan. Ketentuan pada pasal 47 ini memberikan suatu justifikasi, khususnya pada Ayat (1) bahwa TNI dapat menduduki jabatan yang salah satunya dibidang siber negara serta ayat (2) yang memberikan legitimasi hukum terhadap kedudukan rangkap jabatan pada prajurit TNI. Pasal tersebut dapat berimplikasi pada terbukanya ruang terhadap kewenangan TNI yang tanpa batas sehingga hal ini kemudian memberikan suatu akibat pada akses prajurit TNI

19 Hidayat Chusnul Chotimah, *Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]*, Jurnal Politika Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional 10, no. 2, (2019), hal 120-122

20 Chella Defa Anjelina dan Irawan Sapto Adhi, "Apa Isi UU TNI Terbaru? Ini Daftar Lengkap Pasal Yang Berubah," *Kompas.Com*, 2025, <https://www.kompas.com/tren/read/2025/03/20/134500965/apa-isi-uu-tni-terbaru-ini-daftar-lengkap-pasal-yang-berubah>, diakses pada 10 April 2025

untuk melakukan tindakan yang *Abuse Of Power*, hal ini selaras terhadap apa yang dikemukakan oleh Lord Acton "*Power tends to corrupt and absolute power corrupts absolutely*"²¹. Yang dapat ditafsirkan bahwa kekuasaan yang tidak terbatas pasti akan disalahgunakan. Selain itu juga dengan hadirnya Pasal 47 ini dapat memberikan suatu jalan bagi TNI untuk dapat mengambil jabatan strategis di bidang siber dalam tingkatan tertinggi sehingga hal ini dapat berakibat terjadinya peralihan pada bidang siber yang dapat dipimpin oleh TNI sehingga apabila ditafsirkan lebih jauh kedepan, maka ancaman potensial yang dapat terjadi yaitu terjadinya kepemimpinan TNI yang mengambil alih sipil khususnya dibidang siber.

Hal tersebut dapat dilihat secara lebih eksplisit Pada Pasal 7 ayat (2) huruf b angka 15, dengan frasanya "membantu" dalam menghadapi ancaman pertahanan siber. Frasa tersebut secara normatif menempatkan TNI seharusnya sebagai pihak ketiga yang berperan mendukung lembaga terkait dalam hal ini BSSN. Namun, pemaknaan tersebut dapat terderogasi dengan hadirnya frasa "dibukanya ruang bagi TNI untuk menduduki jabatan", pemaknaan tersebut dapat menjadi pintu masuk bagi TNI untuk dapat menjadi pihak utama, bukan lagi pihak yang harus berkoordinasi dengan lembaga yang berwenang, dalam hal ini BSSN.

Padaahal, sebelum hadirnya Revisi Undang-Undang TNI, Penempatan TNI sebagai pihak ketiga telah sesuai dengan amanat dari UUD NRI 1945. Secara lebih mendalam amanat tersebut dapat dilihat pada dua hal utama, yaitu:

1. Supremasi sipil dalam sistem demokrasi Indonesia.

Sistem demokrasi Indonesia menempatkan supremasi sipil sebagai prinsip utama. Apabila kewenangan TNI dalam ruang siber tidak dibatasi secara tegas, hal ini berpotensi mengancam prinsip tersebut. Militer sejatinya adalah alat pertahanan negara yang harus berada di bawah kendali sipil. Ketidadaan batasan yang jelas justru berisiko membalikkan keadaan, di mana militer dapat digunakan sebagai instrumen pemerintah untuk mengontrol masyarakat sipil.²²

2. Prinsip pembatasan kekuasaan sebagai ciri negara hukum.

Dalam negara hukum, setiap lembaga memiliki fungsi untuk saling mengawasi dan membatasi agar tidak melampaui kewenangan yang dimiliki. Dalam konteks ruang siber, prinsip ini menuntut adanya mekanisme hukum, administratif, dan teknis yang memastikan keterlibatan militer hanya sebatas peran yang ditentukan. Dengan demikian, lembaga sipil tetap memiliki kapasitas mengawasi tindakan militer sehingga potensi penyalahgunaan kekuasaan dapat dihindari. Pembagian serta pembatasan fungsi ini menjadi dasar terciptanya sistem *Checks And Balances* yang menjaga keseimbangan kekuasaan.²³

Pasal 47 Revisi Undang-Undang TNI juga menciptakan ruang abu-abu dalam tata kelola keamanan siber nasional, hal ini karena dapat menempatkan TNI sebagai pilar utama dalam hal kewenangan siber, sedangkan BSSN juga memiliki

21 Marzuki, L. (2011). Konstitusionalisme dan Hak Asasi Manusia. *Jurnal Konstitusi*, Vol 8.No 4, Hal 485.

22 Zahidah Dina Firdausi dan Yusa Djuyandi, "Hubungan Politik, Polisi Dan Militer Terhadap Perkembangan Demokrasi Di Indonesia Pada Era Reformasi," *Aliansi : Jurnal Politik, Keamanan Dan Hubungan Internasional* 3, no. 1 (2024): 1–10, <https://doi.org/10.24198/aliansi.v3i1.52252>. hlm. 3-4.

23 Sri Soemantri Martosoewignjo, "Fungsi Konstitusi Dalam Pembatasan Kekuasaan," *Jurnal Hukum Ius Quia Iustum* 3, no. 6 (2016): 1–6, <https://journal.uir.ac.id/IUSTUM/article/view/4919>. Hlm. 2.

kewenangan yang sama sebagai garda terdepan dalam bidang siber. Sehingga hal ini memberikan kewenangan yang tumpang tindih antara TNI dan BSSN dalam hal deteksi, penanggulangan, hingga pemulihan insiden siber dapat menimbulkan fragmentasi kebijakan, dualisme komando, serta ketidakefisienan dalam respons terhadap ancaman siber. Hal ini bertentangan dengan prinsip koordinasi dan efisiensi pemerintahan yang menjadi bagian dari asas umum pemerintahan yang baik (AUPB), dan sekaligus mengancam prinsip *civilian supremacy* dalam sistem demokrasi konstitusional Indonesia. Dari sudut pandang hukum tata negara, perluasan peran militer ke dalam sektor yang sebelumnya sepenuhnya dikelola oleh sipil ini juga mengundang kekhawatiran atas potensi pelanggaran prinsip pemisahan fungsi antara militer dan sipil sebagaimana diamanatkan dalam Pasal 30 UUD 1945 dan filosofis reformasi sektor keamanan pasca-Orde Baru.

Kekhawatiran ini bukan semata-mata bersifat teoritis. Ketika tidak ada delineasi yang jelas antara “keamanan siber” sebagai domain sipil dan “pertahanan siber” sebagai domain militer, maka dapat terjadi tumpang tindih otoritas dalam pelaksanaan fungsi negara, khususnya dalam pengawasan ruang digital publik. Potensi militerisasi ruang siber, terutama apabila prajurit aktif diberi kewenangan dalam pengelolaan ruang digital sipil, juga menimbulkan risiko pelanggaran hak asasi manusia, seperti hak atas privasi, kebebasan berekspresi, dan akses atas informasi.

b. Batasan Intervensi Militer Dalam Demokrasi Digital Demi Melindungi Hak Hak Digital Warga Negara Indonesia

Pembangunan demokrasi kini menjadi agenda utama dalam transformasi politik global. Namun, kemajuan teknologi digital dalam beberapa dekade terakhir telah menghadirkan tantangan serta peluang baru bagi sistem demokrasi. Kehadiran era digital mengubah pola interaksi, komunikasi, dan partisipasi masyarakat dalam ranah politik. Melalui internet, media sosial, dan teknologi analisis data, penyebaran informasi menjadi lebih cepat dan meluas, yang secara mendasar mempengaruhi dinamika demokrasi. Sejatinya dalam sistem demokrasi kedaulatan tertinggi dalam suatu Negara diduduki oleh kedaulatan rakyat, sehingga peran masyarakat menjadi sangat krusial. Demokrasi menawarkan kebebasan dalam berpendapat, pengambilan keputusan yang inklusif, partisipatif, dan akuntabel yang menekankan pada hak asasi manusia dan keadilan sosial.

Pasal 1 ayat (2) UUD NRI 1945 menyatakan secara tegas bahwa kedaulatan tertinggi Negara Indonesia berada ditangan rakyat dan kedaulatan ini dilaksanakan berdasarkan UUD NRI 1945. Hak-hak warga Negara Indonesia telah diatur di dalam pasal 28 secara komprehensif yang meliputi hak untuk berkumpul, mengeluarkan pikiran secara tertulis maupun lisan, dan hak untuk menyatakan pikiran/pendapat dan sikap sesuai hati nuraninya serta hak lainnya. Dimasa digital sekarang pemenuhan hak tersebut tidak hanya dilakukan secara konvensional melainkan juga mencakup ranah digital. Oleh karena itu hak setiap orang yang telah diatur dalam pasal 28 UUD NRI 1945 tidak hanya melekat dalam kehidupan secara langsung namun juga dalam kehidupan digital.

Demokrasi digital merupakan konsep yang relatif baru untuk menggambarkan keterkaitan antara penggunaan media sosial, pemenuhan representasi dan penyaluran

aspirasi, serta peran pemerintah untuk melindungi hak digital warganya. Ketiga elemen ini menjadi komponen krusial dalam memahami dinamika sosial-politik Indonesia saat ini, di mana media sosial mulai berperan sebagai pilar kelima demokrasi, menyusul peran pers.²⁴ Demokrasi membutuhkan ruang sipil yang bebas dan terbuka, termasuk di dunia digital.

Jika dilihat secara lebih mendalam bahwa pada dasarnya ancaman siber terbagi menjadi dua, yaitu serangan siber dan kejahatan siber. Serangan siber adalah tindakan yang bertujuan mengganggu atau merusak jaringan dengan menitikberatkan pada aspek logika dari suatu sistem informasi. Sementara itu, kejahatan siber atau *Cybercrime* dipahami sebagai perbuatan melanggar hukum yang dilakukan melalui perangkat teknologi informasi yang terhubung dengan internet dan dimanfaatkan sebagai sarana untuk melakukan berbagai jenis tindak kriminal. Idealnya militer hanya boleh untuk terlibat dalam penanganan kejahatan siber.²⁵ Jika militer terlalu masuk ke ranah yang menitikberatkan di luar kejahatan siber (misalnya, keterlibatan melakukan pengawasan massal atau operasi siber ofensif di ruang sipil), maka hal ini dapat mengintervensi adanya ruang-ruang kebebasan berekspresi, privasi, dan partisipasi warga. Intervensi militer dalam siber bisa menjadi ancaman terhadap prinsip inklusivitas dan partisipasi, karena bisa menimbulkan rasa takut, pembungkaman, atau pembatasan akses terhadap informasi. Dalam merancang kebijakan dan strategi demokrasi digital, peran militer harus ditempatkan secara proporsional dan terbatas, hanya untuk menghadapi ancaman nyata seperti serangan dari aktor negara atau kelompok teroris siber, bukan untuk mengontrol wacana publik. Pendekatan holistik dan adaptif berarti melibatkan berbagai aktor (sipil, pemerintah, swasta, dan komunitas) dalam menjaga keamanan siber, bukan hanya menyerahkannya kepada militer.²⁶

Sebagaimana yang kita pahami bahwa kelompok militer memiliki sistem peradilan sendiri, hal ini menciptakan *Barrier* bagi anggota militer ketika mereka melakukan pelanggaran untuk dilakukan penindakan secara hukum. Pada dasarnya militer seharusnya hanya digunakan sebagai alat pertahanan keamanan Negara dan melindungi kepentingan rakyat. Namun ketika militer diberi akses untuk mengawasi rakyat secara berlebih dalam hal ini di ranah siber, maka hal ini dapat mengancam kebebasan masyarakat dan bisa jadi diikuti oleh tindakan represif oleh militer.

Dalam konteks keamanan nasional sekarang, pendekatan konvensional yang hanya menekankan pada pertahanan militer di medan perang (*battlefield*) semakin dianggap tidak relevan. Kini, keamanan nasional juga mencakup ruang-ruang sosial, politik, dan budaya yang disebut sebagai *battlespace* seperti media, ruang publik digital, dan wacana masyarakat. Namun militer tidak boleh bertindak secara sewenang-wenang di ruang-ruang ini, karena bisa mengganggu kebebasan berekspresi dan hak sipil warga negara. Demokrasi di era digital mengandalkan keterbukaan, partisipasi publik, dan kebebasan informasi, sehingga jika militer masuk terlalu jauh ke dalam ruang-ruang

24 Dr. Fayakhun Andriadi, *Demokrasi Digital*, "Demokrasi di Tangan Netizen", RM Books Jakarta, Kompas, (Maret 2017), hal. 24

25 Satya Muhammad Sutra dan Agus Haryanto, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal* 7, no. 1 (2023): 56-69, <https://doi.org/10.34010/gpsjournal.v7i1>. hlm. 60.

26 Aulia Ningtyas, *Pembangunan Demokrasi Di Era Digital: Tantangan Dan Prospek*, Fakultas Ilmu Sosial dan Politik, Universitas Medan Area, (Indonesia, 2023), hal. 2-3

digital ini, ia berpotensi menekan kebebasan sipil atas nama keamanan nasional.²⁷ Konsep keamanan nasional yang saat ini justru menuntut keterlibatan masyarakat sipil, media, dan aktor non-negara. Oleh karena itu, peran militer harus dibatasi secara normatif dan operasional, agar tidak mengerdilkan demokrasi yang sedang dibangun di ruang digital.

Demokrasi di Indonesia dibangun berdasarkan UUD NRI 1945 yang menjunjung prinsip kedaulatan rakyat. Konsep ini didasarkan pada tiga hal utama, yaitu nilai-nilai Pancasila, penerapannya dalam sistem pemerintahan, dan komitmen terhadap Pancasila dan UUD NRI 1945. Fokus utamanya adalah penghormatan terhadap HAM serta kesetaraan hak dan martabat setiap warga negara. Untuk menjamin demokrasi, keadilan, dan perlindungan HAM, negara hukum harus ditegakkan. Konstitusi harus melindungi kebebasan HAM, membatasi kekuasaan pemerintah, dan memastikan adanya pengawasan yang ketat terhadap penggunaan kekuasaan tersebut.²⁸

Di tengah urgensi penguatan pertahanan negara di era transformasi digital, penting untuk tetap menempatkan prinsip-prinsip demokrasi sebagai landasan utama dalam merumuskan batas peran militer di ruang siber. Pembentukan Angkatan Siber dan Digital dalam organisasi TNI sebagaimana diusulkan oleh sejumlah akademisi, termasuk Nurmaida Delviana, perlu ditempatkan secara hati-hati agar tidak bertabrakan dengan nilai supremasi sipil yang menjadi karakter utama negara demokratis seperti Indonesia. Negara lain seperti Singapura memang telah membentuk *Digital Intelligence Service* (DIS) yang berfokus pada peperangan digital dan intelijen siber. Namun, model tersebut hanya berhasil karena dibarengi dengan sistem pengawasan ketat, integrasi sipil-militer yang proporsional, dan regulasi hukum yang matang.

Angkatan militer seharusnya hanya menjadi pihak ketiga dalam bidang keamanan siber sehingga angkatan militer dan angkatan siber haruslah dipisahkan. BSSN adalah lembaga utama yang berfungsi sebagai koordinator keamanan siber nasional, namun posisinya saat ini masih lemah secara hukum. Padahal, dengan semakin tersebar nya fungsi-fungsi siber di banyak kementerian dan lembaga seperti Kominfo, Kemenhan, dan bahkan TNI diperlukan satu lembaga pusat yang kuat dan sah secara hukum untuk memastikan sinergi, koordinasi, dan tidak tumpang tindih kewenangan. Indonesia sebagai Negara yang menjunjung tinggi supremasi sipil seharusnya lembaga sipil lah yang menjadi pemimpin dan pengatur utama keamanan siber, sedangkan aktor lain (termasuk militer) hanya berperan sebagai pendukung atau pelaksana teknis, bukan sebagai pemegang kendali utama. Indonesia belum memiliki aturan yang tegas soal akuntabilitas prajurit TNI yang melanggar hukum di ruang sipil, sehingga perlu dihindari fungsi keamanan siber tidak jatuh pada dominasi militer, yang berisiko menciptakan kekebalan hukum dan represi terhadap ruang demokrasi digital.²⁹

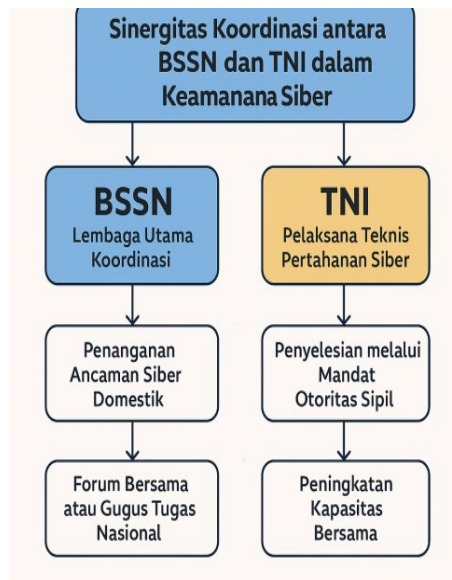
Dalam hal ini BSSN seharusnya berperan sebagai lembaga koordinator utama

27 Kazan Gunawan, Irwan Abdullah, Heru Nugroho, *Human Security Dalam Negara Demokrasi: Perspektif Media Studies*, Volume 1 No. 2, (Kawistara, 2011), hal. 155

28 Dwi Restu Tanjung, Nikmah Dalimunthe, *Sistem Demokrasi Di Indonesia Ditinjau Dari Sudut Hukum Ketatanegaraan*, Universitas Islam Negeri Sumatera Utara, *Journal Of Social Science Research*, Volume 3 Nomor 6, (2023), hal. 7326

29 Nurmaida Delviana, *Inisiasi Pembentukan Angkatan Siber Dan Digital Dalam Organisasi Tentara Nasional Indonesia*, Sekolah Tinggi Hukum Militer, Syntax Admiration, Vol.5, No.2, (Jakarta, 2024), hal. 398

yang menjaga keamanan siber nasional, sedangkan TNI (dalam hal ini Angkatan Siber TNI, jika dibentuk) berperan sebagai pelaksana teknis pertahanan siber yang bersifat defensif, khususnya terhadap ancaman dari luar negeri, seperti serangan dari aktor negara atau kelompok teroris internasional. Posisi BSSN bersifat sipil dan strategis, sedangkan TNI bersifat militer dan taktis. Untuk memahami hal tersebut kami akan kami gambarkan dalam bentuk bagan.



Gambar 1.1 Sinergitas koordinasi BSSN dan TNI yang ideal

Penanganan ancaman siber domestik seperti hoaks, ujaran kebencian, dan peretasan terhadap data pribadi warga negara berada di bawah tanggung jawab lembaga-lembaga sipil seperti Kominfo dan Polri. TNI hanya dilibatkan dalam konteks dukungan teknis dan operasi bersifat defensif aktif dalam skenario yang melibatkan ancaman berskala tinggi terhadap infrastruktur strategis negara (*critical infrastructure*). Unit-unit siber TNI harus diintegrasikan secara terbuka dalam sistem pertahanan siber nasional, bukan menjadi entitas otonom yang menjalankan fungsi pengawasan siber secara independen. Setiap keterlibatan TNI dalam ruang siber sipil harus melalui mandat atau instruksi dari otoritas sipil seperti Presiden atau Menkopolhukam melalui koordinasi dengan BSSN.

2. Dampak Potensial dari Perluasan Fungsi TNI Dalam Bidang Keamanan Siber Terhadap Hak Digital Warga Negara Indonesia

a. Militerisasi Ruang Siber dan Represi Terhadap Kebebasan Digital

Akses terhadap media digital menjadi sangat dominan dalam kehidupan masyarakat. Kehadiran ruang siber telah mentransformasi cara individu dan kelompok berinteraksi dengan negara.³⁰ Ruang siber tidak dapat dipisahkan dari hak-hak sipil dan politik yang dijamin dalam konstitusi dan berbagai instrumen hak asasi manusia, seperti kebebasan berekspresi, hak atas informasi, dan hak untuk berpartisipasi dalam pemerintahan.³¹

³⁰ Paulus Barekama Tukan, *Demokrasi Dalam Ruang Siber Sebagai Tatanan Dunia Baru*, AKADEMIKA 19, no. 1 (2021), hal 61.

³¹ Khairunnisa Supriandi and Wahyu Utama Putra, *Hak Asasi Manusia Di Ranah Digital: Analisis Hukum Siber Dan Kebebasan Online*, Jurnal Hukum Dan HAM Wara Sains 2, no. 08 (2023), hal 691.

Pasal 28 Undang-Undang Dasar 1945 secara jelas dan tegas menjamin kebebasan sipil. Oleh karena itu, pendekatan negara terhadap ruang siber harus mencerminkan pengakuan bahwa ranah ini merupakan bagian dari wilayah sipil, bukan semata-mata ruang teknis atau domain pertahanan-keamanan nasional.

Jika kita melihat jejak histori ketika militer dimasukan kedalam ke ranah sipil, maka kita dapat bandingkan sebagaimana yang terjadi pada masa orde baru. Sejak Proklamasi 17 Agustus 1945, TNI yang kala itu masih bernama Tentara Keamanan Rakyat (TKR) telah mengambil peran sentral dalam mempertahankan eksistensi negara dari ancaman eksternal maupun disintegrasi internal Situasi tersebut membentuk fondasi historis yang menempatkan militer sebagai pilar utama keberlangsungan negara, sehingga secara *de facto* melegitimasi keterlibatannya dalam urusan sosial politik bangsa.

Indonesia dalam masapascakemerdekaan seringkali dihadapkan pada situasi politik yang tidak stabil, ditandai oleh pergolakan ideologis, fragmentasi kekuasaan, serta krisis kepemimpinan sipil. Dalam kekosongan otoritas politik yang efektif, militer menemukan ruang untuk memperluas perannya ke ranah pemerintahan. Gagasan “Jalan Tengah” yang dikembangkan oleh Jenderal A.H. Nasution pada tahun 1950-an mencerminkan strategi kompromi antara tuntutan profesionalisasi militer dan kebutuhan stabilitas nasional. Doktrin ini kemudian menjadi landasan konseptual dari apa yang dikenal sebagai Dwifungsi ABRI, yaitu peran ganda militer sebagai kekuatan pertahanan sekaligus kekuatan sosial politik³². Meskipun pada permukaannya bertujuan untuk mengakomodasi peran strategis militer dalam pembangunan bangsa, pada praktiknya doktrin ini melemahkan prinsip *civilian supremacy over the military*, yang seharusnya menjadi dasar dalam sistem pemerintahan demokratis dan negara hukum.

Dominasi militer dalam ruang sipil sepanjang sejarah Indonesia telah menunjukkan dampak buruk terhadap demokrasi dan hak asasi manusia. Pada masa Orde Baru, kekuasaan militer yang hegemonik melahirkan pemerintahan represif, dengan pembungkaman oposisi, kontrol media, dan pembatasan kebebasan berpendapat. Warga negara kehilangan ruang untuk berekspresi secara bebas, sementara media massa dikendalikan sebagai alat legitimasi kekuasaan.³³

Revisi Undang-Undang TNI yang memperluas fungsi militer ke domain siber memunculkan kekhawatiran akan berulangnya pola represi serupa dalam bentuk baru. Meski menggunakan instrumen teknologi modern, substansi pendekatan militeristik terhadap perbedaan pendapat tetap dipertahankan. Tindakan represif terhadap pembuat konten yang dianggap melemahkan kepercayaan publik terhadap pemerintah menunjukkan bahwa ruang siber kini dimanfaatkan sebagai arena kontrol politik dan pembungkaman ekspresi.

Institusional militer yang memiliki karakteristik mendasar yang tidak sejalan dengan prinsip pemerintahan sipil. Pertama, militer dibentuk dan dididik untuk menggunakan kekerasan sebagai alat utama dalam penyelesaian konflik, sebuah pendekatan yang bertentangan dengan prinsip deliberatif dalam pengambilan kebijakan publik. Kedua,

³² Clara Venia Leilafatkur Rizqi, *Pemikiran AH Nasution Tentang Dwifungsi ABRI Tahun 1958-1998*, (2020), hal 17.

³³ Safenet Voice, “Kembalikan Militer ke Barak, Hentikan Militerisasi Ruang Siber!”, <https://safenet.or.id/id/2025/03/kembalikan-militer-ke-barak-hentikan-militerisasi-ruang-siber/>, diakses pada 11 April 2025

loyalitas militer yang bersifat tunggal kepada negara seringkali diterjemahkan sebagai loyalitas kepada rezim yang berkuasa, yang dapat mengaburkan garis demarkasi antara kepentingan negara dan kepentingan politik tertentu. Ketiga, struktur hierarkis dan budaya senioritas dalam militer tidak memberikan ruang bagi proses diskursif dan partisipatif yang menjadi ciri khas dari pemerintahan demokratis yang berbasis pada akuntabilitas dan transparansi³⁴.

Peran TNI dalam sistem pertahanan dan keamanan negara harus senantiasa diletakkan dalam kerangka konstitusional yang membedakan secara tegas fungsi pertahanan yang menjadi domain TNI. Dalam masa damai, pelibatan TNI ke dalam ranah sipil harus dilakukan secara terbatas dan proporsional, serta tunduk pada prinsip-prinsip hukum dan demokrasi. Penggunaan sumber daya nasional oleh TNI hanya dapat dibenarkan apabila telah berada dalam status dinas aktif, yang secara hukum menandai dimulainya fungsi operasional pertahanan negara. Oleh karena itu, dalam konteks masa damai, TNI tidak memiliki kewenangan untuk melakukan pembinaan terhadap sumber daya nasional yang masih berstatus sipil. Pelibatan TNI dalam fungsi keamanan domestik hanya dapat dilakukan apabila terdapat keadaan luar biasa yang secara tegas diatur dalam peraturan perundang-undangan. Semua ini harus dijalankan dengan tetap menjunjung tinggi hak-hak sipil dan menegakkan supremasi sipil.³⁵

b. Demokrasi di ruang Digital Setelah RUU TNI

Pasca disahkannya Revisi Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (UU TNI) pada 20 Maret 2025, kewenangan TNI secara resmi diperluas ke domain siber, khususnya dalam operasi militer selain perang (OMSP) untuk menanggulangi ancaman pertahanan siber dan melindungi infrastruktur kritis nasional. Perubahan ini menuai sorotan tajam dari masyarakat sipil, akademisi, dan organisasi advokasi hak digital, karena dinilai berpotensi menimbulkan tumpang tindih kewenangan dengan lembaga-lembaga sipil seperti Badan Siber dan Sandi Negara (BSSN), serta membuka ruang bagi pendekatan militeristik dalam pengelolaan ruang digital yang selama ini berada di bawah regulasi sipil.

Saat ini memang belum ada tindakan represif yang secara terang bisa dikatakan sebagai akibat dari disahkannya RUU TNI tersebut sebab RUU tersebut belum genap dua bulan disahkan. Namun di beberapa pemberitaan kita bisa melihat bahwa ruang gerak masyarakat semakin diawasi di dunia digital, hal ini bisa kita lihat di sosial media yang beredar bahwa ada sekelompok diduga anggota aparat penegak hukum yang mendatangi tempat tinggal salah satu netizen yang sempat mengkritik pemerintah di media. Berita tersebut memang belum ada kepastiannya, namun hal ini memunculkan kekhawatiran masyarakat untuk menyuarakan pendapat di media sosial.

Ruang siber, yang kini dipandang sebagai arena “perang informasi” dan “perang opini,” semakin mudah dijadikan ladang operasi militer. Di bawah narasi stabilitas dan keamanan nasional, kontrol terhadap informasi dan opini publik berisiko menjadi instrumen penindasan terhadap oposisi politik dan pembungkaman media. Ketika militer mulai mengambil alih fungsi-fungsi sipil dalam tata kelola informasi, demokrasi

³⁴ Sidratahta Mukhtar, *Militer Dan Demokrasi*, (malang: intrans publishing, 2017), hal 60.

³⁵ Sidratahta Mukhtar, hal 76-77.

digital yang seharusnya menjamin hak-hak digital warga negara, seperti kebebasan berekspresi dan hak atas informasi.

KESIMPULAN

Tata kelola keamanan siber di Indonesia harus mengutamakan supremasi sipil, dengan BSSN memimpin pengelolaan ruang digital dan TNI dibatasi hanya untuk pertahanan terhadap ancaman eksternal berskala besar. RUU TNI 2025 yang memperluas kewenangan TNI di siber harus dibarengi dengan pemisahan yang jelas antara keamanan siber sipil dan militer untuk mencegah tumpang tindih dan pelanggaran hak digital warga negara. Ruang siber harus tetap terbuka untuk kebebasan berekspresi dan partisipasi publik, dengan intervensi militer dibatasi oleh hukum dan kontrol sipil yang ketat.

Perluasan fungsi TNI ke bidang keamanan siber dapat mengancam hak digital warga negara, mengingat karakter militer yang tidak sesuai dengan prinsip demokrasi dan perlindungan hak asasi manusia. Sejarah keterlibatan militer dalam ranah sipil, seperti masa Orde Baru, menunjukkan potensi pembatasan kebebasan berekspresi dan kontrol media. Meskipun belum ada tindakan represif yang signifikan pasca-revisi UU TNI, meningkatnya pengawasan digital menimbulkan kekhawatiran terhadap kebebasan berekspresi. Oleh karena itu, pelibatan TNI dalam keamanan siber harus dibatasi pada keadaan luar biasa dan selalu berada di bawah kontrol sipil.

DAFTAR PUSTAKA

- 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 (2023): 63–66.
- Aulia Ningtyas, *Pembangunan Demokrasi di Era Digital: Tantangan dan Prospek* (Medan: Fakultas Ilmu Sosial dan Politik, Universitas Medan Area, 2023), 2–3.
- Badan Siber dan Sandi Negara, “Tentang BSSN,” n.d., <https://www.bssn.go.id/tentang-bssn/> (diakses April 11, 2025).
- Berita Borneo, “Seusai UU TNI Disahkan: Bagaimana Kewenangan TNI di Dunia Siber?,” n.d., <https://beritaborneo.com/main/seusai-uu-tni-disahkan-bagaimana-kewenangan-tni-di-dunia-siber/> (diakses April 15, 2025).
- Chella Defa Anjelina dan Irawan Sapto Adhi, “Apa Isi UU TNI Terbaru? Ini Daftar Lengkap Pasal yang Berubah,” *Kompas.com*, Maret 20, 2025, <https://www.kompas.com/tren/read/2025/03/20/134500965/apa-isi-uu-tni-terbaru-ini-daftar-lengkap-pasal-yang-berubah> (diakses April 10, 2025).
- Clara Venia Leilafatkur Rizqi, *Pemikiran AH Nasution tentang Dwifungsi ABRI Tahun 1958–199
- Dwi Restu Tanjung dan Nikmah Dalimunthe, “Sistem Demokrasi di Indonesia Ditinjau dari Sudut Hukum Ketatanegaraan,” *Journal of Social Science Research* 3, no. 6 (2023): 7326.
- Fayakhun Andriadi, *Demokrasi Digital: Demokrasi di Tangan Netizen* (Jakarta: RM

- Books Kompas, 2017), 24.
- GINANJAR, M. F. FIRDAUSYI, S. SUSWANDY, dan N. T. ANDINI, “Perlindungan HAM dalam Era Digital: Tantangan dan Solusi Hukum,” *Journal on Education* 4, no. 4 (2022): 2084.
- GOODKIND, “RUU TNI Disahkan: Pengamat – Ruang Digital Warga Akan Dikontrol Kekuasaan,” n.d., <https://goodkind.id/tulisan/ruu-tni-disahkan-pengamat-ruang-digital-warga-akan-dikontrol-oleh-kekuasaan/> (diakses April 22, 2025).
- HIDAYAT CHUSNUL CHOTIMAH, “Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara,” *Jurnal Politica* 10, no. 2 (2019): 120–122.
- HUKUM UMA, “Evolusi Hukum Pidana di Era Digital: Tantangan dan Peluang,” September 6, 2024, <https://hukum.uma.ac.id/2024/09/06/evolusi-hukum-pidana-di-era-digital-tantangan-dan-peluang/> (diakses April 10, 2025).
- ID-SIRTII, “Badan Siber dan Sandi Negara,” n.d., <https://idsirtii.or.id/bssn.html> (diakses April 10, 2025).
- KAZAN GUNAWAN, IRWAN ABDULLAH, dan HERU NUGROHO, “Human Security dalam Negara Demokrasi: Perspektif Media Studies,” *Kawistara* 1, no. 2 (2011): 155.
- KHAIRUNNISA SUPRIANDI dan WAHYU UTAMA PUTRA, “Hak Asasi Manusia di Ranah Digital: Analisis Hukum Siber dan Kebebasan Online,” *Jurnal Hukum dan HAM Wara Sains* 2, no. 08 (2023): 691.
- KOMPAS, “Sipil dan Militer dalam Penjagaan Ruang Siber,” April 2, 2025, <https://nasional.kompas.com/read/2025/04/02/08061311/sipil-dan-militer-dalam-penjagaan-ruang-siber?page=all> (diakses April 29, 2025).
- MARZUKI, “Konstitusionalisme dan Hak Asasi Manusia,” *Jurnal Konstitusi* 8, no. 4 (2011): 485.
- MEDIA INDONESIA, “SAFEnet: Revisi UU TNI Berdampak pada Militerisasi Ruang Siber, Hak Digital Publik Akan Terancam,” Maret 29, 2025, <https://mediaindonesia.com/politik-dan-hukum/753532/safenet-revisi-uu-tni-berdampak-pada-militerisasi-ruang-siber-hak-digital-publik-akan-terancam> (diakses Maret 29, 2025).
- NASUTION, “Hak Kebebasan Berpendapat dan Berekspresi dalam Ruang Publik di Era Digital,” *Adalah* 4, no. 3 (2020): 38.
- NURMAIDA DELVIANA, “Inisiasi Pembentukan Angkatan Siber dan Digital dalam Organisasi Tentara Nasional Indonesia,” *Jurnal Syntax Admiration* 5, no. 2 (2024): 397.
- NURMAIDA DELVIANA, “Inisiasi Pembentukan Angkatan Siber dan Digital dalam Organisasi Tentara Nasional Indonesia,” *Syntax Admiration* 5, no. 2 (Jakarta: Sekolah Tinggi Hukum Militer, 2024), 398.
- PAULUS BAREKAMA TUKAN, “Demokrasi dalam Ruang Siber sebagai Tatahan Dunia Baru,” *Akademika* 19, no. 1 (2021): 61.
- PDM MARZUKI, *Penelitian Hukum: Edisi Revisi* (Jakarta: Prenada Media, 2017), 54.
- PUSPITASARI, “Perlindungan Hak Asasi Digital,” *Sekretariat Kabinet Republik Indonesia*, Agustus 13, 2022, <https://setkab.go.id/perlindungan-hak-asasi-digital/> (diakses

April 10, 2025).

Reda Manthovani, *Penyadapan vs. Privasi* (Jakarta: PT Bhuana Ilmu Populer, 2013), 35.

Republik Indonesia, *Undang-Undang Nomor 3 Tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional*.

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

Shabrina S., “Jumlah Pengguna Internet Indonesia Tembus 229 Juta pada 2025,” *Teknologi.id*, Agustus 7, 2025, <https://teknologi.id/tekno/apjii-rilis-data-terbaru-2025-pengguna-internet-di-indonesia-capai-229-juta-jiwa> (diakses Agustus 17, 2025).

Sri Soemantri Martosoewignjo, “Fungsi Konstitusi dalam Pembatasan Kekuasaan,” *Jurnal Hukum Ius Quia Iustum* 3, no. 6 (2016): 1–6, <https://journal.uui.ac.id/IUSTUM/article/view/4919>.

Syafiul Hadi, “Wiranto Akan Resmikan Badan Siber dan Sandi Negara Bulan Ini,” *Tempo*, 2017, <https://www.tempo.co/politik/wiranto-akan-resmikan-badan-siber-dan-sandi-negara-bulan-ini-1156991> (diakses April 11, 2025).

Zahidah Dina Firdausi dan Yusa Djuyandi, “Hubungan Politik, Polisi dan Militer terhadap Perkembangan Demokrasi di Indonesia pada Era Reformasi,” *Aliansi: Jurnal Politik, Keamanan dan Hubungan Internasional* 3, no. 1 (2024): 1–10, <https://doi.org/10.24198/aliansi.v3i1.52252>.