SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

REGULATORY LAG DAN REFORMASI REGULASI KEAMANAN NASIONAL INDONESIA DALAM MENGHADAPI ANCAMAN MULTIDOMAIN

Rio Akmal Syahbana[1*]
[1]Sekolah Tinggi Ilmu Hukum Manokwari Papua Barat, Indonesia
*Email: **rioakmal97@gmail.com**

Korespondensi penulis: ***rioakmal97@gmail.com***

Abstract. *Contemporary security threats have shifted national security from a traditional military-oriented agenda toward a multidomain problem involving cyber risks, data protection, critical infrastructure, geoeconomics, supply chains, energy resilience, disinformation, and socio-political stability. Indonesia's national security regulation, however, remains largely rooted in the early Reformasi design that separates defence, domestic security, and military functions into sectoral legal frameworks. This article analyses the forms of regulatory lag in Indonesia's national security governance, assesses the state's political will in regulatory and institutional reform, and formulates an adaptive, integrative, and democratic reform model. The study applies a qualitative method using normative-juridical, conceptual, and policy analysis approaches. Data are drawn from legislation, national development planning documents, institutional reports, global risk reports, and academic literature on security studies, cybersecurity governance, security sector governance, and civil-military relations. The findings show that regulatory lag is reflected in misaligned threat definitions, fragmented authority, weak integration of cyber-data-critical infrastructure governance, and insufficient inter-agency coordination mechanisms. The state's political will has emerged through the National Defence Council, cybersecurity strategy, vital information infrastructure protection, the 2025-2029 RPJMN, and the amendment to the TNI Law, yet these measures remain partial. The article proposes an Adaptive-Integrative-Democratic National Security Model that strengthens security effectiveness while preserving civilian supremacy, democratic accountability, and the rule of law.*

Keywords: *cybersecurity; defence governance; national security; regulatory lag; regulatory reform*

Abstrak. Perkembangan ancaman keamanan kontemporer telah menggeser keamanan nasional dari orientasi militer-tradisional menuju persoalan multidomain yang mencakup siber, data, infrastruktur kritis, geoekonomi, rantai pasok, energi, disinformasi, dan stabilitas sosial-politik. Namun, kerangka regulasi keamanan nasional Indonesia masih banyak bertumpu pada desain awal Reformasi yang memisahkan pertahanan negara, keamanan dalam negeri, dan tugas militer secara sektoral. Artikel ini bertujuan menganalisis bentuk regulatory lag dalam keamanan nasional Indonesia, menilai political will negara dalam pembaruan regulasi dan kelembagaan, serta merumuskan model reformasi regulasi yang adaptif, integratif, dan demokratis. Penelitian menggunakan metode kualitatif dengan pendekatan normatif-yuridis, konseptual, dan analisis kebijakan. Data diperoleh dari peraturan perundang-undangan, dokumen RPJMN, laporan BPHN, laporan risiko global, serta literatur security studies, cybersecurity governance, security sector governance, dan civil-military relations. Hasil penelitian menunjukkan bahwa regulatory lag tampak pada ketidaksinkronan definisi ancaman, fragmentasi kewenangan, lemahnya integrasi siber-data-infrastruktur kritis, dan belum mapannya mekanisme koordinasi lintas kementerian/lembaga. Political will negara telah muncul melalui DPN, strategi keamanan siber, pelindungan infrastruktur informasi vital, RPJMN 2025-2029, dan perubahan UU TNI, tetapi masih parsial. Artikel ini menawarkan Model Keamanan Nasional Adaptif-Integratif-Demokratis sebagai kerangka reformasi yang menjaga efektivitas keamanan, supremasi sipil, akuntabilitas demokratis, dan prinsip negara hukum.

Kata kunci: keamanan nasional; keamanan siber; regulatory lag; reformasi regulasi; tata kelola pertahanan

1. LATAR BELAKANG

Keamanan nasional merupakan konsep yang selalu bergerak mengikuti perubahan lingkungan strategis, perkembangan teknologi, dan transformasi hubungan antara negara, masyarakat, pasar, serta aktor nonnegara. Dalam tradisi klasik, keamanan nasional cenderung ditempatkan sebagai persoalan kelangsungan hidup negara, ancaman militer, strategi

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

pertahanan, dan penggunaan instrumen koersif. Walt (1991) menempatkan studi keamanan pada pertanyaan tentang ancaman militer dan cara negara menggunakan kekuatan untuk mempertahankan kepentingannya. Cara pandang tersebut tidak salah dalam konteks Perang Dingin, tetapi menjadi semakin terbatas ketika ancaman yang dihadapi negara tidak lagi hanya berbentuk agresi bersenjata. Setelah Perang Dingin, keamanan berkembang sebagai agenda yang lebih luas. Baldwin (1995) mengajukan perlunya meninjau ulang objek, nilai, instrumen, dan aktor keamanan, sedangkan Buzan (1991) memperluas sektor keamanan ke ranah militer, politik, ekonomi, sosial, dan lingkungan. Buzan dan Hansen (2009) kemudian menjelaskan bahwa evolusi studi keamanan bergerak dari fokus strategis-militer menuju perluasan agenda yang lebih kompleks. Dalam tradisi critical security studies, Booth (2005) bahkan menekankan keamanan sebagai pembebasan manusia dan masyarakat dari ancaman yang membatasi kehidupan, martabat, dan kebebasannya.

Perluasan konseptual tersebut menjadi sangat relevan dalam situasi global mutakhir. Ancaman keamanan tidak hanya datang melalui invasi militer, tetapi juga melalui serangan siber, kebocoran data, sabotase infrastruktur kritis, disinformasi digital, tekanan geoekonomi, perang dagang, gangguan rantai pasok, krisis energi, migrasi tidak teratur, polarisasi sosial, bencana kesehatan, dan manipulasi teknologi baru. Williams dan McDonald (2023) serta Collins (2025) menempatkan teknologi baru, keamanan siber, energi, migrasi, kesehatan, dan infrastruktur kritis sebagai bagian dari spektrum keamanan kontemporer. World Economic Forum (2026) juga menggambarkan risiko global sebagai jaringan krisis yang saling terhubung, mencakup ketidakstabilan geopolitik, disrupsi teknologi, tekanan lingkungan, dan kerentanan sosial. International Monetary Fund (IMF, 2025) menilai ekonomi global masih berada dalam ketahanan yang rapuh di tengah ketidakpastian, sementara SIPRI (2026) mencatat peningkatan belanja militer dunia pada 2025 yang menunjukkan bahwa negara-negara semakin memberi perhatian pada risiko geopolitik dan keamanan. Dengan kata lain, keamanan nasional abad ke-21 adalah keamanan yang bersifat multidomain, lintas sektor, lintas aktor, dan lintas batas.

Di Indonesia, perubahan lanskap ancaman tersebut belum sepenuhnya diikuti oleh pembaruan regulasi keamanan nasional yang komprehensif. Arsitektur hukum keamanan nasional masih banyak dipengaruhi oleh desain awal Reformasi, terutama melalui Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, dan Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia. Secara historis, desain tersebut memiliki arti penting karena menata ulang hubungan sipil-militer, membatasi warisan dwifungsi ABRI, memisahkan fungsi pertahanan dan keamanan dalam negeri, serta mengembalikan militer ke ranah profesional pertahanan negara. Namun, ketika ancaman semakin bersifat siber, digital, ekonomi, informasi, dan infrastruktur, pemisahan sektoral yang terlalu kaku mulai memunculkan ruang abu-abu kewenangan. Serangan terhadap pusat data, sistem pembayaran, jaringan energi, pelabuhan, sistem transportasi, layanan kesehatan, atau platform informasi publik sulit dikategorikan secara sederhana sebagai urusan pertahanan, keamanan dalam negeri, administrasi pemerintahan, atau perlindungan data semata. (Indonesia, 2002a, 2002b, 2004).

Kondisi tersebut dapat dibaca melalui konsep regulatory lag. Regulatory lag merujuk pada keadaan ketika perkembangan ancaman, teknologi, praktik sosial, atau kebutuhan tata kelola bergerak lebih cepat daripada kemampuan regulasi untuk menyesuaikan diri. Dalam konteks keamanan nasional, regulatory lag bukan hanya berarti belum adanya aturan baru,

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

tetapi juga mencakup ketidaksesuaian definisi ancaman, tumpang tindih kewenangan, kekosongan mekanisme koordinasi, lemahnya standar resiliensi, serta tidak adanya mekanisme evaluasi regulasi yang berkala. Ahern (2021) menggunakan istilah regulatory lag untuk menjelaskan bagaimana perubahan teknologi dapat membuat regulasi tertinggal, menimbulkan friksi, dan memerlukan transisi regulatif. Dalam konteks Indonesia, regulatory lag terlihat ketika kerangka hukum dasar masih bekerja dengan logika pertahanan-keamanan yang sektoral, sementara ancaman kontemporer bergerak melalui jejaring digital, ekonomi, infrastruktur, dan psikososial yang saling berkelindan.

Negara sebenarnya tidak pasif. Sejumlah kebijakan terbaru menunjukkan adanya political will untuk merespons ancaman kontemporer. Peraturan Presiden Nomor 202 Tahun 2024 membentuk Dewan Pertahanan Nasional sebagai lembaga nonstruktural yang dipimpin Presiden dan diberi tugas memberi pertimbangan serta merumuskan solusi kebijakan pertahanan nasional strategis. Di bidang siber, Peraturan Presiden Nomor 47 Tahun 2023 mengatur Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, sedangkan Peraturan Presiden Nomor 82 Tahun 2022 mengatur Pelindungan Infrastruktur Informasi Vital. RPJMN 2025-2029 juga menempatkan keamanan dan ketahanan siber sebagai agenda pembangunan nasional. Perubahan Undang-Undang TNI melalui Undang-Undang Nomor 3 Tahun 2025 menunjukkan adanya pembaruan sebagian norma mengenai kedudukan dan peran TNI. Akan tetapi, keseluruhan langkah tersebut belum otomatis membentuk desain keamanan nasional yang integratif, demokratis, dan operasional lintas kementerian/lembaga. (Bappenas, 2025; Indonesia, 2022b, 2023, 2024, 2025a, 2025b).

Dalam perspektif kebijakan publik, masalah ini tidak boleh dipersempit menjadi persoalan teknis peraturan perundang-undangan. Regulatory lag menunjukkan adanya jarak antara kecepatan perubahan ancaman dan kapasitas negara untuk memperbarui aturan, institusi, serta prosedur kerja. Jarak tersebut dapat mengakibatkan respons yang lambat, penggunaan kewenangan yang tidak sinkron, duplikasi program, dan lemahnya akuntabilitas ketika krisis terjadi. Karena itu, pembaruan regulasi keamanan nasional perlu dibaca sebagai agenda reformasi tata kelola negara, bukan semata-mata agenda sektor pertahanan atau keamanan. Artikel ini menempatkan hukum sebagai instrumen pengarah koordinasi, pembatas kekuasaan, dan penguat resiliensi nasional.

Berdasarkan latar belakang tersebut, artikel ini menjawab tiga pertanyaan penelitian. Pertama, mengapa regulasi keamanan nasional Indonesia dapat dikategorikan mengalami regulatory lag dalam menghadapi ancaman multidomain? Kedua, bagaimana political will negara dalam merespons kebutuhan pembaruan regulasi dan kelembagaan keamanan nasional? Ketiga, model reformasi regulasi apa yang dapat dirumuskan agar keamanan nasional Indonesia lebih adaptif, integratif, dan demokratis? Kebaruan artikel ini terletak pada upaya menghubungkan regulatory lag, political will, dan reformasi regulasi keamanan nasional dalam satu kerangka analisis. Berbeda dari tulisan yang hanya menempatkan keamanan nasional sebagai isu ancaman atau isu hukum sektoral, artikel ini membaca ketertinggalan regulasi sebagai gejala struktural yang lahir dari ketidaksinkronan antara perubahan ancaman, desain kelembagaan, dan arah pembaruan hukum. Artikel ini juga menawarkan Model Keamanan Nasional Adaptif-Integratif-Demokratis sebagai kontribusi konseptual dan rekomendatif bagi reformasi tata kelola keamanan nasional Indonesia.

Dengan posisi tersebut, artikel ini tidak bermaksud mengusulkan kembalinya paradigma keamanan yang sentralistik, melainkan menyusun cara berpikir baru yang mampu mempertemukan efektivitas negara dan pembatasan kekuasaan. Reformasi keamanan nasional

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

harus menjawab kebutuhan praktis menghadapi ancaman cepat, tetapi tetap menempatkan hukum sebagai pagar demokrasi. Oleh karena itu, setiap rekomendasi dalam artikel ini diarahkan pada peningkatan koherensi regulasi, bukan perluasan kewenangan tanpa batas. Tekanan analisis diberikan pada kesesuaian antara konsep ancaman, desain institusi, mekanisme koordinasi, dan prinsip akuntabilitas.

2. TINJAUAN PUSTAKA

2.1 Regulatory Lag dan Tata Kelola Adaptif

Regulatory lag menggambarkan keadaan ketika perubahan teknologi, pola ancaman, dan praktik sosial bergerak lebih cepat daripada kapasitas hukum untuk menetapkan definisi, kewenangan, standar, dan mekanisme pertanggungjawaban yang relevan. Ahern (2021) menunjukkan bahwa ketertinggalan regulasi tidak hanya menghasilkan kekosongan aturan, tetapi juga regulatory friction dan fragmentasi ketika pembaruan dilakukan secara parsial. Dalam artikel ini, konsep tersebut diadaptasi untuk membaca arsitektur keamanan nasional: hukum dapat tetap tersedia dalam jumlah besar, tetapi kehilangan daya integrasinya ketika setiap aturan bekerja dalam logika sektoral yang berbeda.

Perspektif agile governance menekankan perlunya regulasi dan organisasi publik yang mampu belajar, menyesuaikan prosedur, serta memperbarui kebijakan berdasarkan perubahan risiko. Nilai adaptivitas tidak identik dengan deregulasi, melainkan menuntut siklus evaluasi, mekanisme umpan balik, dan kemampuan mengoreksi kebijakan secara cepat tanpa mengabaikan legalitas. Kajian Tomaževič et al. (2023) memperlihatkan bahwa digitalisasi akan lebih mendukung tata kelola yang baik apabila disertai nilai-nilai agile, terutama pengelolaan perubahan, pelayanan yang berfungsi, dan penguatan hubungan internal organisasi.

2.2 Tata Kelola Siber, Data, dan Infrastruktur Kritis

Literatur cybersecurity governance memandang keamanan siber sebagai persoalan kelembagaan dan kebijakan, bukan sekadar persoalan teknis. Atkins dan Lawson (2021) menunjukkan bahwa kebijakan infrastruktur kritis yang bersifat patchwork menghasilkan capaian yang tidak merata karena keberhasilan sangat dipengaruhi tekanan regulatif, karakter ancaman, dan kapasitas organisasi. Dalam konteks Indonesia, Aji (2025), Ananta et al. (2025), dan Fajar et al. (2025) sama-sama menyoroti fragmentasi kewenangan, ketidakpastian regulasi, serta kebutuhan penguatan koordinasi BSSN, Polri, TNI, kementerian teknis, dan penyelenggara infrastruktur digital. Temuan tersebut sejalan dengan Aryanti (2025) dan Mishra et al. (2022) yang menempatkan kepemimpinan, kebijakan, manajemen risiko, serta budaya organisasi sebagai unsur utama ketahanan siber.

2.3 Supremasi Sipil dan Akuntabilitas Demokratis

Reformasi regulasi keamanan nasional harus tetap berpijak pada prinsip security sector governance. Pengalaman demokratisasi menunjukkan bahwa penguatan kapasitas keamanan tanpa pembatasan kewenangan berisiko mendorong sekuritisasi, perluasan ruang intervensi, dan pelemahan kontrol sipil. Stojanović-Gajić dan Pavlović (2021) menekankan hubungan antara tata kelola sektor keamanan dan risiko state capture dalam rezim hibrida, sedangkan Taş (2024) menunjukkan bahwa dinamika populisme dapat memengaruhi hubungan sipil-militer. Dalam konteks Indonesia, profesionalisme militer dan batas peran institusional tetap menjadi fondasi penting Reformasi (Djuyandi et al., 2025). Karena itu, orientasi resiliensi harus

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

memperkuat demokrasi melalui riset, pendidikan, pengawasan, dan kapasitas institusi sipil, bukan menggantikan supremasi sipil dengan sentralisasi koersif (Tagarev & Fluri, 2025).

3. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan normatif-yuridis, pendekatan konseptual, dan analisis kebijakan. Pendekatan normatif-yuridis digunakan karena objek utama penelitian adalah norma hukum dan desain kelembagaan yang mengatur keamanan nasional Indonesia. Regulasi yang dianalisis meliputi Undang-Undang Nomor 2 Tahun 2002 tentang Polri, Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, Undang-Undang Nomor 34 Tahun 2004 tentang TNI, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Peraturan Presiden Nomor 202 Tahun 2024 tentang Dewan Pertahanan Nasional, Peraturan Presiden Nomor 12 Tahun 2025 tentang RPJMN 2025-2029, serta Undang-Undang Nomor 3 Tahun 2025 tentang perubahan UU TNI. Regulasi tersebut dipilih karena mewakili simpul utama pengaturan pertahanan, keamanan dalam negeri, militer, data, siber, infrastruktur kritis, perencanaan pembangunan, dan kelembagaan strategis negara.

Pendekatan konseptual digunakan untuk membaca hubungan antara perubahan konsep keamanan dan kebutuhan pembaruan regulasi. Literatur yang digunakan meliputi security studies, critical security studies, security sector governance, cybersecurity governance, agile governance, dan civil-military relations. Konsep regulatory lag digunakan sebagai kerangka utama untuk menjelaskan ketertinggalan regulasi, sedangkan political will digunakan untuk menilai keseriusan negara dalam menerjemahkan kesadaran ancaman menjadi regulasi, kelembagaan, agenda perencanaan, dan mekanisme koordinasi. Analisis kebijakan digunakan untuk membaca apakah produk hukum dan dokumen perencanaan yang telah diterbitkan negara telah membentuk desain operasional yang memadai atau masih berhenti pada pembaruan parsial.

Data penelitian terdiri atas bahan hukum primer, bahan hukum sekunder, dan dokumen kebijakan. Bahan hukum primer berupa peraturan perundang-undangan dan peraturan presiden yang relevan. Bahan hukum sekunder berupa buku, artikel jurnal, laporan penelitian, dan kajian akademik mengenai keamanan nasional, keamanan siber, tata kelola sektor keamanan, dan hubungan sipil-militer. Dokumen kebijakan meliputi laporan BPHN tentang evaluasi hukum pertahanan negara, agenda evaluasi keamanan siber, dokumen RPJMN 2025-2029, laporan World Economic Forum, laporan IMF, dan data SIPRI. Teknik pengumpulan data dilakukan melalui studi kepustakaan dan telaah dokumen. Semua data dibaca secara tematik untuk menemukan pola pengaturan, kekosongan norma, tumpang tindih kewenangan, indikasi political will, dan arah pembaruan regulasi. Dokumen evaluasi hukum digunakan untuk memperkuat identifikasi masalah normatif dan kelembagaan (Badan Pembinaan Hukum Nasional, 2024, 2025).

Teknik analisis dilakukan melalui empat tahap. Pertama, identifikasi norma untuk memetakan fungsi, kewenangan, dan cakupan pengaturan masing-masing regulasi. Kedua, analisis regulatory lag dengan indikator ketidaksesuaian definisi ancaman, fragmentasi kewenangan, kekosongan mekanisme koordinasi, lemahnya integrasi data-siber-infrastruktur kritis, dan tidak adanya evaluasi regulasi berkala. Ketiga, analisis political will dengan indikator pembentukan lembaga, penerbitan regulasi baru, penempatan isu dalam RPJMN, dan

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

kejelasan mekanisme implementasi. Keempat, perumusan model preskriptif melalui sintesis antara temuan normatif, perkembangan konsep keamanan, dan prinsip demokrasi. Validitas analisis dijaga melalui triangulasi sumber, yaitu membandingkan regulasi, dokumen kebijakan, laporan lembaga, dan literatur akademik. Penelitian ini bersifat normatif-preskriptif sehingga tidak mengukur efektivitas implementasi secara kuantitatif, tetapi menyusun argumentasi reformasi berdasarkan kebutuhan hukum dan tata kelola keamanan kontemporer.

Untuk menjaga konsistensi analisis, setiap regulasi dibaca melalui tiga pertanyaan kerja. Pertama, ancaman apa yang diasumsikan oleh regulasi tersebut dan apakah asumsi itu masih relevan dengan ancaman multidomain. Kedua, aktor mana yang diberi kewenangan dan bagaimana hubungan kewenangan tersebut dengan aktor lain. Ketiga, apakah regulasi menyediakan mekanisme implementasi, pengawasan, dan evaluasi. Tiga pertanyaan ini membantu artikel membedakan antara keberadaan regulasi dan kecukupan regulasi. Dengan cara demikian, temuan tidak berhenti pada daftar peraturan, tetapi bergerak pada penilaian apakah peraturan tersebut mampu membentuk tata kelola keamanan nasional yang koheren.

Tabel 1. Indikator Analisis Penelitian

Aspek Analisis	Indikator Operasional	Fungsi dalam Penelitian
Regulatory lag	Ketidaksesuaian definisi ancaman; fragmentasi kewenangan; kekosongan mekanisme koordinasi; lemahnya integrasi siber-data-infrastruktur kritis; tidak adanya evaluasi berkala.	Menilai bentuk ketertinggalan regulasi keamanan nasional.
Political will	Pembentukan lembaga; penerbitan regulasi baru; penempatan isu dalam RPJMN; kejelasan implementasi; pembagian tanggung jawab.	Menilai keseriusan negara dalam merespons perubahan ancaman.
Reformasi regulasi	Integrasi normatif; koordinasi strategis; tata kelola risiko; akuntabilitas demokratis; evaluasi adaptif.	Merumuskan model preskriptif yang dapat mengurangi regulatory lag.

Sumber: Diolah penulis (2026).

4. HASIL DAN PEMBAHASAN

4.1 Regulatory Lag sebagai Ketertinggalan Arsitektural

Hasil penelitian menunjukkan bahwa regulatory lag dalam keamanan nasional Indonesia tidak dapat dipahami sebagai kekosongan regulasi total. Indonesia memiliki banyak instrumen hukum yang mengatur pertahanan, kepolisian, militer, data pribadi, infrastruktur informasi vital, keamanan siber, perencanaan pembangunan, dan kelembagaan pertahanan strategis. Masalah utamanya bukan absennya regulasi, melainkan fragmentasi, ketidakterpaduan, dan belum adanya kerangka yang secara utuh menghubungkan ancaman multidomain ke dalam tata kelola keamanan nasional. Dengan demikian, regulatory lag Indonesia lebih tepat disebut sebagai ketertinggalan arsitektural, yaitu kondisi ketika kerangka hukum tersedia secara sektoral, tetapi belum mampu bekerja sebagai sistem keamanan nasional yang terintegrasi, adaptif, dan akuntabel. Pola ini konsisten dengan konsep regulatory lag dan fragmentasi kebijakan yang dijelaskan Ahern (2021).

Secara konseptual, regulatory lag dalam artikel ini dibaca melalui lima indikator. Pertama, ketidaksesuaian definisi ancaman, yaitu ketika regulasi masih membedakan ancaman secara konvensional sementara realitas ancaman bergerak lintas domain. Kedua, fragmentasi kewenangan, yaitu ketika banyak aktor memiliki kewenangan terkait, tetapi tidak terdapat desain koordinasi yang jelas. Ketiga, kekosongan mekanisme operasional, yaitu ketika regulasi sudah memberikan arah kebijakan tetapi belum memuat protokol kerja, pembagian tanggung

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

jawab, sistem berbagi informasi, dan prosedur krisis yang teruji. Keempat, lemahnya integrasi siber, data, dan infrastruktur kritis ke dalam konsepsi keamanan nasional. Kelima, belum adanya mekanisme evaluasi regulasi berkala yang memungkinkan hukum diperbarui sebelum tertinggal dari perubahan teknologi dan ancaman. Kelima indikator tersebut digunakan untuk membaca regulasi keamanan nasional Indonesia.

Temuan pertama adalah adanya ketidaksesuaian antara desain awal Reformasi dan karakter ancaman multidomain. UU Polri, UU Pertahanan Negara, dan UU TNI dibangun dalam konteks demokratisasi pasca-Orde Baru. Agenda utamanya adalah membatasi dominasi militer, memisahkan peran pertahanan dan keamanan dalam negeri, serta menegakkan supremasi sipil. Dalam konteks historis, desain tersebut sangat penting dan harus tetap dihormati. Namun, tantangan keamanan abad ke-21 tidak selalu dapat ditempatkan secara tegas dalam batas institusional tersebut. Serangan siber terhadap layanan publik, kebocoran data penduduk, sabotase sistem energi, manipulasi informasi, gangguan rantai pasok pangan, serangan terhadap pusat data nasional, dan disrupsi sistem pembayaran dapat berdampak pada keamanan nasional tanpa harus berbentuk agresi militer konvensional. Peristiwa semacam itu menuntut respons yang melibatkan BSSN, Komdigi, Polri, TNI, Kementerian Pertahanan, kementerian teknis, pemerintah daerah, penyelenggara sistem elektronik, badan usaha, dan masyarakat.

UU Pertahanan Negara sebenarnya telah mengenal ancaman militer dan nonmiliter. Namun, pengaturan operasional ancaman nonmiliter belum cukup rinci untuk menjawab kompleksitas siber, data, infrastruktur digital, geoekonomi, dan ketahanan rantai pasok. UU TNI menempatkan TNI sebagai alat pertahanan negara, sementara UU Polri menempatkan Polri sebagai alat negara yang memelihara keamanan dan ketertiban masyarakat serta menegakkan hukum. Kedua norma ini bekerja penting dalam batas sektoral masing-masing. Persoalannya muncul ketika ancaman memerlukan respons campuran: penegakan hukum digital, pemulihan layanan publik, perlindungan infrastruktur strategis, pertahanan siber, diplomasi siber, dan komunikasi krisis publik. Dalam situasi tersebut, pembagian tugas sektoral perlu didampingi oleh mekanisme koordinasi nasional yang jelas agar tidak terjadi tumpang tindih, saling menunggu, atau saling klaim kewenangan.

Temuan kedua adalah fragmentasi regulasi dalam isu siber, data, dan infrastruktur kritis. Indonesia telah memiliki Undang-Undang Pelindungan Data Pribadi, Perpres Pelindungan Infrastruktur Informasi Vital, dan Perpres Strategi Keamanan Siber Nasional serta Manajemen Krisis Siber. Ketiganya menunjukkan perkembangan penting. Namun, hubungan ketiganya dengan kerangka keamanan nasional belum sepenuhnya mapan. Data pribadi diatur sebagai hak subjek data dan kewajiban pengendali atau prosesor data, tetapi data juga memiliki nilai strategis bagi negara. Infrastruktur informasi vital diatur sebagai objek yang harus diidentifikasi, dilindungi, dibina, diawasi, dan dikoordinasikan, tetapi mekanisme integrasinya dengan pertahanan nasional, penegakan hukum, dan manajemen krisis lintas sektor masih memerlukan penguatan. Strategi keamanan siber nasional memberi arah dan acuan, tetapi posisinya sebagai Perpres membuatnya bergantung pada konsistensi implementasi, kapasitas lembaga, dan koordinasi lintas aktor. Kajian mutakhir tentang politik keamanan siber Indonesia juga menunjukkan problem ketidakpastian regulasi dan integrasi kelembagaan (Aji, 2025; Ananta et al., 2025; Fajar et al., 2025).

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

4.2 Peta Regulasi dan Fragmentasi Kewenangan

Indikator pertama, yaitu ketidaksesuaian definisi ancaman, tampak ketika regulasi lama masih menempatkan ancaman dalam kategori yang relatif stabil, sedangkan ancaman kontemporer bergerak secara cair. Ancaman siber dapat berawal dari aktor kriminal, tetapi berdampak pada layanan publik dan ketahanan nasional. Disinformasi dapat muncul sebagai aktivitas digital warga, tetapi jika terkoordinasi secara sistematis dapat melemahkan legitimasi negara dan stabilitas sosial. Tekanan geoekonomi dapat berbentuk kebijakan dagang, tetapi berdampak pada pasokan energi, pangan, industri pertahanan, dan stabilitas harga. Kategori ancaman yang terlalu kaku membuat negara kesulitan menentukan ambang respons dan aktor penanggung jawab. Karena itu, reformasi regulasi perlu merumuskan definisi ancaman yang fungsional, berbasis dampak, dan tetap memiliki batas hukum yang jelas.

Indikator kedua, yaitu fragmentasi kewenangan, tidak hanya terjadi karena banyaknya lembaga, tetapi juga karena belum kuatnya desain hubungan antarlembaga. Dalam tata kelola modern, banyaknya aktor tidak selalu menjadi masalah apabila terdapat protokol koordinasi, mekanisme pertukaran data, sistem komando-koordinasi, dan standar evaluasi bersama. Masalah muncul ketika setiap aktor bekerja berdasarkan mandat sendiri tanpa forum pemadu yang efektif. Dalam konteks keamanan nasional, fragmentasi semacam ini dapat menyebabkan keterlambatan respons, perbedaan interpretasi ancaman, dan kesulitan menentukan akuntabilitas. Oleh sebab itu, harmonisasi regulasi harus diikuti desain operasional yang menjawab pertanyaan siapa melakukan apa, kapan, berdasarkan dasar hukum apa, dan kepada siapa bertanggung jawab.

Indikator ketiga, yaitu kekosongan mekanisme operasional, menjadi pembeda antara regulasi yang bersifat deklaratif dan regulasi yang benar-benar dapat dijalankan. Banyak regulasi memberikan arah umum, tetapi tidak selalu mengatur mekanisme kerja ketika krisis terjadi. Dalam ancaman multidomain, prosedur operasional menjadi penting karena krisis biasanya bergerak cepat dan menuntut keputusan lintas sektor. Misalnya, dalam serangan terhadap pusat data layanan publik, negara harus menentukan status insiden, memulihkan layanan, melindungi data, menegakkan hukum, mengelola komunikasi publik, dan mencegah eskalasi politik. Tanpa protokol terintegrasi, respons dapat berjalan terpisah-pisah dan memunculkan persepsi bahwa negara tidak siap.

Indikator keempat, yaitu lemahnya integrasi siber-data-infrastruktur kritis, menunjukkan bahwa keamanan nasional digital tidak cukup diurus melalui satu sektor. Data pribadi adalah hak warga, tetapi kebocoran data dalam skala besar juga dapat memengaruhi kepercayaan publik dan keamanan negara. Infrastruktur informasi vital adalah objek teknis, tetapi gangguan terhadapnya dapat melumpuhkan layanan publik, transaksi ekonomi, transportasi, kesehatan, dan komunikasi. Keamanan siber adalah domain teknologi, tetapi juga terkait diplomasi, hukum pidana, pertahanan, dan tata kelola pemerintahan. Karena itu, regulasi harus membangun jembatan antarsektor agar setiap insiden dapat dinilai berdasarkan dampak nasionalnya, bukan hanya berdasarkan asal sektornya.

Indikator kelima adalah ketiadaan evaluasi adaptif. Perubahan teknologi dan pola ancaman berlangsung lebih cepat daripada siklus legislasi sehingga regulasi cepat tertinggal. Regulatory review, horizon scanning, dan simulasi krisis diperlukan agar negara menutup celah hukum lebih awal sekaligus mencegah kewenangan berlebih. Pembelajaran organisasi harus berlangsung berkelanjutan (Tomaževič et al., 2023).

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

Tabel 2. Peta Regulatory Lag dalam Regulasi Keamanan Nasional Indonesia

Regulasi/Dokumen	Fokus Pengaturan	Bentuk Regulatory Lag	Implikasi
UU No. 2 Tahun 2002 tentang Polri	Keamanan dan ketertiban masyarakat, penegakan hukum, perlindungan, pengayoman, dan pelayanan masyarakat.	Belum cukup mengatur ancaman multidomain seperti siber, data, dan infrastruktur kritis secara integratif.	Memerlukan koordinasi lebih kuat dengan BSSN, TNI, kementerian teknis, dan aktor nonnegara.
UU No. 3 Tahun 2002 tentang Pertahanan Negara	Pertahanan negara, sistem pertahanan semesta, ancaman militer dan nonmiliter.	Ancaman nonmiliter telah dikenal, tetapi pengaturan operasional lintas sektor belum memadai.	Perlu pembaruan norma agar pertahanan terhubung dengan keamanan siber, ekonomi, dan infrastruktur kritis.
UU No. 34 Tahun 2004 jo. UU No. 3 Tahun 2025 tentang TNI	Kedudukan, tugas, dan peran TNI sebagai alat pertahanan negara.	Perlu kejelasan batas peran TNI dalam ancaman nonperang, siber, dan ruang sipil.	Harus dikawal dengan supremasi sipil, akuntabilitas, dan pembatasan kewenangan.
UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi	Hak subjek data, kewajiban pengendali/prosesor data, sanksi, dan kelembagaan.	Belum sepenuhnya terhubung dengan keamanan nasional dan perlindungan infrastruktur kritis.	Data pribadi perlu dipahami sekaligus sebagai hak warga dan aset strategis nasional.
Perpres No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital	Identifikasi, pelindungan, pembinaan, pengawasan, dan koordinasi IIV.	Efektivitas bergantung pada implementasi sektor dan koordinasi antarlembaga.	Perlu penguatan standar, audit, pelaporan insiden, dan latihan krisis.
Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber	Arah strategi keamanan siber nasional dan mekanisme manajemen krisis siber.	Belum setingkat undang-undang dan belum menyelesaikan semua potensi tumpang tindih kewenangan.	Menjadi indikator political will, tetapi memerlukan konsolidasi hukum dan kelembagaan.
Perpres No. 202 Tahun 2024 tentang Dewan Pertahanan Nasional	Pertimbangan dan perumusan solusi kebijakan pertahanan nasional strategis.	Fokus normatifnya pada pertahanan nasional, belum menjadi kerangka keamanan nasional menyeluruh.	Berpotensi menjadi simpul strategis, tetapi memerlukan kejelasan hubungan kerja lintas K/L.
Perpres No. 12 Tahun 2025 tentang RPJMN 2025-2029	Arah pembangunan nasional, termasuk keamanan dan ketahanan siber.	Dokumen perencanaan belum otomatis menyelesaikan fragmentasi hukum.	Menjadi dasar agenda, tetapi perlu peta jalan regulasi dan implementasi.

Sumber: Diolah penulis (2026).

Fragmentasi tersebut dapat dilihat dari banyaknya aktor yang terlibat dalam keamanan siber. BSSN memiliki peran strategis dalam keamanan siber dan sandi negara. Polri berperan dalam penegakan hukum tindak pidana siber. TNI dapat memiliki peran pertahanan siber dalam konteks pertahanan negara. Komdigi dan kementerian teknis terkait memiliki kewenangan dalam tata kelola sistem elektronik dan sektor masing-masing. Pemerintah daerah mengelola layanan publik digital dan sebagian infrastruktur pelayanan masyarakat. Badan usaha, terutama penyelenggara sistem elektronik dan pengelola infrastruktur strategis, memegang aset digital yang menjadi bagian dari resiliensi nasional. Tanpa desain koordinasi yang tegas, ancaman siber berpotensi diperlakukan sebagai isu teknis, isu hukum, isu pertahanan, atau isu administrasi secara terpisah, padahal dampaknya dapat menjadi krisis nasional.

4.3 Political Will Negara: Ada, tetapi Parsial

Temuan ketiga adalah political will negara telah muncul, tetapi belum terkonsolidasi. Political will dapat dilihat dari pembentukan lembaga, penerbitan regulasi, penempatan isu dalam dokumen perencanaan, dan kejelasan mekanisme koordinasi. Pada indikator pertama, pembentukan Dewan Pertahanan Nasional melalui Perpres Nomor 202 Tahun 2024 menunjukkan kehendak negara untuk memperkuat pemberian pertimbangan dan perumusan

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

solusi kebijakan pertahanan nasional strategis. DPN dipimpin Presiden, memiliki anggota tetap dan tidak tetap, serta diarahkan pada isu kedaulatan negara, keutuhan wilayah, dan keselamatan bangsa. Posisi ini penting karena menunjukkan perlunya forum strategis tingkat tinggi untuk membaca ancaman dan memberi masukan kebijakan. Namun, DPN secara normatif tetap berada pada bidang pertahanan nasional, bukan otomatis menjadi lembaga keamanan nasional dalam arti luas. Karena itu, perannya perlu dibaca hati-hati: DPN dapat menjadi simpul koordinasi strategis, tetapi penguatan fungsinya harus tetap didasarkan pada mandat hukum yang jelas.

Pada indikator kedua, penerbitan Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber menunjukkan bahwa pemerintah telah menempatkan keamanan siber sebagai agenda strategis. Perpres ini menjadi acuan bagi instansi penyelenggara negara dan pemangku kepentingan untuk membangun kekuatan dan kapabilitas siber dalam rangka stabilitas keamanan siber. Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital juga menunjukkan pengakuan bahwa infrastruktur digital tertentu memiliki nilai vital bagi negara dan masyarakat. Namun, kedua Perpres tersebut masih perlu diperkuat dalam bentuk harmonisasi lintas sektor, standar implementasi, kewajiban pelaporan insiden, audit resiliensi, latihan krisis bersama, dan mekanisme pemulihan yang dapat diuji. Dengan kata lain, political will pada tataran kebijakan telah ada, tetapi perlu diterjemahkan menjadi institusionalisasi yang lebih operasional.

Pada indikator ketiga, RPJMN 2025-2029 menempatkan keamanan dan ketahanan siber dalam agenda pembangunan nasional. Ini penting karena menunjukkan bahwa keamanan siber tidak hanya dipahami sebagai isu teknis lembaga tertentu, tetapi juga sebagai bagian dari pembangunan nasional. Namun, dokumen perencanaan belum otomatis mengatasi fragmentasi regulasi. RPJMN memberi arah, target, dan prioritas pembangunan, sedangkan reformasi regulasi memerlukan harmonisasi norma, pembagian kewenangan, penganggaran, kapasitas sumber daya manusia, pengawasan, dan evaluasi. Dengan demikian, RPJMN dapat menjadi indikator kesadaran negara, tetapi tidak cukup apabila tidak diikuti oleh peta jalan regulasi yang lebih jelas.

Pada indikator keempat, perubahan UU TNI melalui UU Nomor 3 Tahun 2025 menunjukkan bahwa negara melakukan pembaruan terhadap sebagian norma TNI. Namun, pembaruan tersebut belum menyelesaikan persoalan arsitektur keamanan nasional secara keseluruhan. Bahkan, revisi norma militer dalam konteks ancaman nonperang perlu ditempatkan dalam kerangka supremasi sipil dan akuntabilitas demokratis. Pembaruan keamanan nasional tidak boleh dibaca sebagai perluasan kewenangan koersif negara tanpa batas. Jika integrasi keamanan nasional tidak disertai pembatasan kewenangan, mekanisme pengawasan, dan transparansi proporsional, reformasi dapat berubah menjadi sekuritisasi yang mengancam hak warga negara. Karena itu, political will yang dibutuhkan bukan hanya kehendak untuk memperkuat negara, tetapi kehendak untuk memperkuat negara hukum yang mampu bekerja efektif sekaligus demokratis.

Pemetaan regulasi menunjukkan bahwa Indonesia memiliki banyak instrumen yang relevan, tetapi setiap instrumen bergerak dengan logika sektoral. UU Polri memusatkan perhatian pada keamanan dan ketertiban masyarakat serta penegakan hukum. UU Pertahanan Negara mengatur pertahanan negara, sistem pertahanan semesta, dan ancaman militer maupun nonmiliter. UU TNI mengatur kedudukan, tugas, dan peran TNI sebagai alat pertahanan negara. UU Pelindungan Data Pribadi mengatur hak subjek data, kewajiban pengendali data, sanksi, dan kelembagaan pelindungan data. Perpres Pelindungan Infrastruktur Informasi Vital

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

mengatur identifikasi dan pelindungan infrastruktur informasi vital. Perpres Strategi Keamanan Siber Nasional memberikan arah keamanan siber dan manajemen krisis siber. Perpres DPN membentuk forum strategis pertahanan nasional. RPJMN menempatkan keamanan siber sebagai agenda pembangunan. Masing-masing penting, tetapi belum terdapat satu desain yang menjelaskan hubungan antarinstrumen dalam menghadapi krisis multidomain.

Dalam perspektif security sector governance, fragmentasi tersebut berisiko menimbulkan tiga masalah. Pertama, masalah efektivitas, karena respons krisis dapat terlambat apabila aktor tidak memiliki prosedur bersama. Kedua, masalah akuntabilitas, karena tumpang tindih kewenangan dapat menyulitkan penentuan siapa yang bertanggung jawab atas kegagalan pencegahan atau respons. Ketiga, masalah legitimasi, karena publik dapat kehilangan kepercayaan jika negara tampak tidak mampu melindungi data, layanan publik, atau infrastruktur penting. Oleh sebab itu, reformasi regulasi tidak hanya diperlukan untuk memperkuat kewenangan negara, tetapi juga untuk memperjelas tanggung jawab negara. Risiko tersebut sejalan dengan temuan tata kelola infrastruktur kritis bahwa kebijakan yang terfragmentasi dapat menghasilkan keberhasilan dan kegagalan yang tidak merata (Atkins & Lawson, 2021).

Kasus siber menjadi contoh paling nyata. Serangan terhadap infrastruktur digital dapat dimulai sebagai insiden teknis, berkembang menjadi gangguan layanan publik, memunculkan kerugian ekonomi, menimbulkan kegaduhan politik, dan berakhir sebagai krisis kepercayaan terhadap negara. Dalam satu rangkaian kejadian, terdapat unsur teknologi, hukum pidana, perlindungan data, komunikasi publik, diplomasi, keamanan nasional, dan tata kelola krisis. Jika regulasi hanya membagi isu tersebut ke dalam sektor-sektor terpisah, maka respons negara cenderung reaktif. Kerangka adaptif diperlukan agar negara mampu melakukan horizon scanning, penilaian risiko, pencegahan, deteksi dini, respons cepat, pemulihan, dan pembelajaran kelembagaan.

4.4 Risiko Demokrasi, Supremasi Sipil, dan Akuntabilitas

Selain siber, infrastruktur kritis juga memerlukan perhatian. Infrastruktur informasi vital, sistem energi, transportasi, pelabuhan, keuangan, kesehatan, pangan, dan telekomunikasi saling terhubung melalui sistem digital. Gangguan pada satu sektor dapat berdampak berantai pada sektor lain. Dalam logika ini, keamanan nasional tidak dapat dipisahkan dari resiliensi infrastruktur. Resiliensi tidak hanya berarti kemampuan bertahan dari serangan, tetapi juga kemampuan pulih, belajar, dan menyesuaikan diri setelah krisis. Oleh karena itu, regulasi keamanan nasional perlu menghubungkan perlindungan infrastruktur kritis dengan kewajiban audit risiko, pelaporan insiden, standar keamanan minimum, latihan krisis lintas sektor, dan mekanisme pemulihan layanan dasar.

Dalam kaitan dengan DPN, artikel ini menilai bahwa posisi kelembagaan tersebut perlu dilihat secara proporsional. DPN bukan pengganti kementerian/lembaga teknis dan bukan pula badan operasional krisis. Nilai strategis DPN terletak pada kemampuannya memberi pertimbangan dan merumuskan solusi kebijakan pertahanan nasional strategis di tingkat Presiden. Karena itu, DPN dapat berfungsi sebagai forum pemadu perspektif geostrategi, geopolitik, risiko pertahanan, dan keselamatan bangsa. Namun, untuk menghadapi ancaman multidomain yang melibatkan siber, data, ekonomi, dan infrastruktur kritis, DPN memerlukan hubungan kerja yang jelas dengan BSSN, Kementerian Pertahanan, Polri, TNI, Komdigi, Bappenas, Kementerian Dalam Negeri, dan kementerian sektoral lain. Tanpa hubungan kerja yang jelas, potensi strategis DPN tidak otomatis berubah menjadi efektivitas koordinasi.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

Penguatan DPN juga harus menghindari dua ekstrem. Ekstrem pertama adalah menjadikan DPN sekadar forum administratif yang tidak memiliki daya pengaruh terhadap kebijakan strategis. Ekstrem kedua adalah memperluas DPN menjadi pusat komando keamanan nasional yang terlalu luas tanpa dasar hukum memadai. Jalan tengahnya adalah menempatkan DPN sebagai simpul strategic policy advice yang bekerja melalui analisis risiko, rekomendasi lintas sektor, dan penilaian geostrategis, sementara fungsi operasional tetap berada pada kementerian/lembaga sesuai mandatnya. Dengan desain ini, DPN dapat membantu mengurangi regulatory lag pada tingkat strategis tanpa menciptakan tumpang tindih baru.

Regulatory lag juga tampak dalam belum kuatnya mekanisme evaluasi regulasi. Banyak regulasi dibuat sebagai respons terhadap masalah tertentu, tetapi tidak selalu disertai mekanisme evaluasi berkala. Padahal, ancaman teknologi berubah sangat cepat. Dalam lima tahun, pola serangan siber, kecerdasan buatan, deepfake, perang informasi, komputasi awan, rantai pasok perangkat keras, dan ketergantungan data dapat berubah drastis. Jika regulasi tidak dievaluasi secara berkala, maka negara selalu berada dalam posisi tertinggal. Oleh karena itu, reformasi keamanan nasional perlu memasukkan regulatory review setiap tiga sampai lima tahun, horizon scanning ancaman, dan mekanisme pembelajaran lintas lembaga.

Dalam konteks demokrasi, tantangan terbesar adalah membedakan integrasi dari sentralisasi. Integrasi berarti menghubungkan aktor, kewenangan, data, prosedur, dan standar agar negara mampu merespons ancaman secara koheren. Sentralisasi berarti memusatkan kekuasaan secara berlebihan pada satu aktor atau institusi sehingga berpotensi melemahkan pengawasan. Reformasi keamanan nasional Indonesia harus memilih integrasi demokratis, bukan sentralisasi koersif. Integrasi demokratis mengandaikan koordinasi yang kuat, tetapi tetap membatasi kewenangan, membuka pengawasan DPR, menyediakan audit independen, menjaga perlindungan hak warga negara, dan memastikan keterlibatan masyarakat sipil pada isu yang berdampak pada kebebasan sipil.

4.5 Model Keamanan Nasional Adaptif-Integratif-Demokratis

Kajian civil-military relations memperkuat kehati-hatian tersebut. Reformasi sektor keamanan pasca-Orde Baru bertujuan membangun militer profesional, menegakkan supremasi sipil, dan membatasi keterlibatan militer dalam politik. Ketika ancaman nonmiliter dan hibrida meningkat, terdapat kecenderungan negara memperluas peran aktor keamanan ke wilayah sipil. Kecenderungan ini dapat dipahami dari kebutuhan efektivitas, tetapi juga membawa risiko demokrasi jika tidak dikendalikan. Karena itu, pembaruan regulasi keamanan nasional harus mengandung prinsip pembatasan kewenangan, legalitas tindakan, proporsionalitas, kebutuhan yang sah, pengawasan yudisial atau parlementer, serta akuntabilitas publik. Keamanan yang efektif tanpa demokrasi dapat berubah menjadi represif, sedangkan demokrasi tanpa kapasitas keamanan dapat menjadi rentan. Model yang diperlukan adalah keseimbangan keduanya. Kerangka ini selaras dengan literatur yang menempatkan profesionalisme militer, resiliensi demokratis, dan kontrol sipil sebagai unsur yang harus berjalan bersama (Djuyandi et al., 2025; Tagarev & Fluri, 2025).

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

Tabel 3. Model Rekomendasi Reformasi Regulasi Keamanan Nasional Adaptif-Integratif-Demokratis

Masalah Utama	Arah Reformasi	Instrumen yang Diperlukan	Indikator Keberhasilan
Fragmentasi regulasi pertahanan, keamanan, siber, data, dan infrastruktur kritis.	Membangun integrasi normatif keamanan nasional.	Payung hukum atau harmonisasi regulasi keamanan nasional yang demokratis.	Definisi ancaman jelas; tidak ada tumpang tindih kewenangan; hubungan kerja antarlembaga terukur.
Koordinasi lintas K/L belum kuat menghadapi ancaman multidomain.	Memperkuat whole-of-government approach.	Protokol koordinasi krisis, pusat informasi bersama, latihan lintas sektor.	Respons krisis lebih cepat, prosedur teruji, dan evaluasi pascakrisis berjalan.
Keamanan siber belum memiliki payung hukum komprehensif setingkat UU.	Mendorong UU keamanan dan ketahanan siber berbasis hak dan demokrasi.	Pengaturan kewenangan, pelaporan insiden, audit, pemulihan, kerja sama, dan pengawasan.	Peran BSSN, Polri, TNI, Komdigi, sektor privat, dan daerah menjadi jelas.
Pelindungan infrastruktur kritis masih sektoral.	Menghubungkan infrastruktur kritis dengan resiliensi nasional.	Standar nasional resiliensi, audit keamanan, kewajiban pelaporan, dan latihan pemulihan.	Kerentanan menurun dan pemulihan layanan dasar lebih cepat.
Risiko sekuritisasi dan perluasan kewenangan tanpa kontrol.	Menjaga supremasi sipil dan akuntabilitas demokratis.	Pengawasan DPR, audit independen, mekanisme pengaduan, transparansi proporsional, evaluasi HAM.	Reformasi keamanan tidak berubah menjadi represi dan kepercayaan publik meningkat.
Regulasi cepat tertinggal dari ancaman baru.	Membentuk evaluasi adaptif.	Regulatory review 3-5 tahun, horizon scanning, regulatory sandbox teknologi keamanan.	Celah hukum ditutup lebih awal dan kebijakan lebih responsif.

Sumber: Diolah penulis (2026).

Berdasarkan temuan tersebut, artikel ini menawarkan Model Keamanan Nasional Adaptif-Integratif-Demokratis. Model ini dibangun atas tiga asumsi dasar. Pertama, ancaman keamanan nasional kontemporer bersifat multidomain sehingga tidak dapat dijawab oleh satu institusi, satu regulasi, atau satu sektor kebijakan. Kedua, pembaruan regulasi harus mengurangi fragmentasi tanpa menghapus pelajaran Reformasi mengenai supremasi sipil, profesionalisme militer, dan pembatasan kekuasaan koersif. Ketiga, keamanan nasional harus dipahami sebagai tata kelola risiko dan resiliensi, bukan semata-mata mobilisasi kekuatan negara. Dengan tiga asumsi ini, reformasi regulasi diarahkan bukan untuk memperbesar kekuasaan negara secara tidak terbatas, melainkan untuk memperjelas tanggung jawab, memperkuat koordinasi, dan menjaga akuntabilitas.

Komponen pertama model ini adalah integrasi normatif. Integrasi normatif berarti membangun kerangka hukum yang menghubungkan pertahanan negara, keamanan dalam negeri, keamanan siber, pelindungan data, pelindungan infrastruktur kritis, ketahanan ekonomi, dan stabilitas sosial-politik. Integrasi tidak harus selalu berbentuk satu undang-undang tunggal yang menghapus seluruh undang-undang sektoral. Pilihan reformasi dapat berupa undang-undang keamanan nasional yang demokratis, undang-undang keamanan dan ketahanan siber yang komprehensif, harmonisasi undang-undang sektoral, atau peta jalan legislasi yang memastikan tidak ada kekosongan norma. Yang terpenting adalah adanya definisi ancaman yang jelas, pembagian kewenangan yang tegas, dan hubungan kerja lintas aktor yang dapat diuji.

Komponen kedua adalah koordinasi strategis lintas lembaga. Koordinasi strategis diperlukan karena ancaman multidomain tidak mengikuti batas birokrasi. DPN dapat dipertimbangkan sebagai salah satu simpul strategis dalam bidang pertahanan nasional, tetapi penguatan perannya harus ditempatkan dalam mandat yang jelas dan tidak menimbulkan tumpang tindih dengan kementerian/lembaga lain. Untuk isu siber dan infrastruktur kritis,

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

diperlukan protokol koordinasi yang menjelaskan kapan suatu insiden dikategorikan sebagai insiden sektoral, insiden nasional, atau krisis nasional. Protokol ini harus mengatur siapa yang memimpin, siapa yang mendukung, bagaimana informasi dibagi, bagaimana komunikasi publik dilakukan, bagaimana pemulihan dilaksanakan, dan bagaimana evaluasi pascakrisis disusun.

Komponen ketiga adalah tata kelola risiko dan resiliensi. Keamanan nasional tidak boleh hanya reaktif setelah krisis terjadi. Negara perlu membangun siklus kebijakan yang terdiri atas pencegahan, kesiapsiagaan, deteksi dini, respons, pemulihan, dan pembelajaran. Siklus ini dapat diterapkan pada keamanan siber, infrastruktur kritis, rantai pasok, energi, pangan, dan stabilitas sosial. Setiap sektor strategis perlu memiliki penilaian risiko, standar minimum keamanan, kewajiban pelaporan insiden, audit resiliensi, latihan krisis, serta mekanisme pemulihan. Dengan pendekatan resiliensi, keberhasilan keamanan nasional tidak hanya diukur dari kemampuan mencegah serangan, tetapi juga dari kemampuan menjaga layanan dasar dan memulihkan kepercayaan publik.

Komponen keempat adalah akuntabilitas demokratis. Setiap reformasi keamanan nasional harus disertai pengawasan DPR, audit lembaga independen, mekanisme pengaduan publik, transparansi proporsional, perlindungan data pribadi, dan penghormatan terhadap hak asasi manusia. Akuntabilitas demokratis juga berarti bahwa penggunaan kewenangan keamanan harus berbasis hukum, proporsional, dapat diuji, dan tidak digunakan untuk membatasi kritik publik secara sewenang-wenang. Dalam isu siber, misalnya, kewenangan pemantauan dan penanganan insiden harus dibedakan secara tegas dari kewenangan pengawasan warga. Negara perlu kuat menghadapi serangan, tetapi tidak boleh menjadikan keamanan siber sebagai alasan untuk memperluas kontrol terhadap ruang sipil tanpa batas.

Komponen kelima adalah evaluasi adaptif. Regulasi keamanan nasional harus memiliki mekanisme pembaruan berkala. Evaluasi dapat dilakukan setiap tiga sampai lima tahun dengan melibatkan pemerintah, DPR, lembaga pengawas, akademisi, pakar teknologi, pelaku industri, dan masyarakat sipil. Evaluasi harus menilai apakah definisi ancaman masih relevan, apakah pembagian kewenangan efektif, apakah protokol krisis bekerja, apakah perlindungan hak warga memadai, dan apakah kapasitas lembaga meningkat. Evaluasi adaptif juga dapat didukung oleh horizon scanning dan regulatory sandbox untuk teknologi tertentu yang berdampak pada keamanan, seperti kecerdasan buatan, komputasi awan, identitas digital, biometrik, dan sistem otomasi pertahanan.

4.6 Agenda Implementasi dan Kontribusi Artikel

Model tersebut dapat diterjemahkan ke dalam beberapa agenda reformasi. Agenda pertama adalah harmonisasi definisi ancaman keamanan nasional. Definisi ancaman harus mencakup ancaman militer, nonmiliter, hibrida, siber, ekonomi, informasi, dan infrastruktur kritis, tetapi tetap dirumuskan secara hati-hati agar tidak menjadi pasal karet. Definisi yang terlalu luas dapat memberi ruang sekuritisasi terhadap masalah sosial biasa. Definisi yang terlalu sempit membuat negara lambat merespons ancaman baru. Karena itu, definisi ancaman perlu dilengkapi indikator dampak, ambang krisis, mekanisme penetapan status, dan prosedur pengawasan.

Agenda kedua adalah penguatan payung hukum keamanan dan ketahanan siber. Perpres keamanan siber telah memberi arah, tetapi Indonesia memerlukan dasar hukum yang lebih kuat untuk mengatur tata kelola siber secara komprehensif. Payung hukum tersebut perlu menjelaskan peran BSSN, Polri, TNI, Komdigi, kementerian teknis, pemerintah daerah, dan

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

sektor privat. Selain itu, aturan harus memuat kewajiban pelaporan insiden, klasifikasi infrastruktur kritis, perlindungan data, mekanisme respons krisis, audit keamanan, standar minimum, kerja sama internasional, dan pengawasan hak asasi manusia. Kekuatan undang-undang diperlukan bukan semata-mata untuk memperbesar kewenangan lembaga, tetapi untuk memperjelas batas dan tanggung jawabnya.

Agenda ketiga adalah penyusunan protokol nasional respons krisis multidomain. Protokol ini harus dapat digunakan ketika terjadi serangan siber besar, gangguan infrastruktur vital, krisis energi, gangguan rantai pasok, atau disinformasi yang mengancam stabilitas sosial. Protokol perlu memuat mekanisme komando-koordinasi, struktur komunikasi krisis, pembagian peran antarlembaga, keterlibatan sektor privat, dan tahap pemulihan. Protokol juga harus diuji melalui latihan bersama secara berkala. Tanpa latihan, regulasi dapat terlihat baik di atas kertas tetapi tidak efektif ketika krisis terjadi.

Agenda keempat adalah penguatan kapasitas kelembagaan. Regulatory lag tidak hanya terjadi karena aturan tertinggal, tetapi juga karena kapasitas implementasi lemah. Penguatan kapasitas meliputi sumber daya manusia, anggaran, teknologi, budaya koordinasi, sistem informasi, dan kemampuan analitik. Kementerian/lembaga perlu memiliki pejabat dan unit yang memahami tata kelola risiko keamanan kontemporer. Pemerintah daerah juga harus dilibatkan karena banyak layanan publik digital dan infrastruktur pelayanan masyarakat berada di tingkat daerah. Keterlibatan daerah penting agar keamanan nasional tidak berhenti sebagai isu pusat, tetapi menjadi ekosistem resiliensi nasional.

Agenda kelima adalah penguatan pengawasan dan partisipasi. Reformasi keamanan nasional harus membuka ruang bagi pengawasan DPR, lembaga negara independen, akademisi, masyarakat sipil, dan media. Tentu tidak semua informasi keamanan dapat dibuka kepada publik, tetapi prinsip transparansi proporsional tetap diperlukan. Publik berhak mengetahui arah kebijakan, standar perlindungan data, mekanisme pengaduan, dan akuntabilitas ketika terjadi kegagalan perlindungan. Kepercayaan publik adalah bagian dari keamanan nasional. Negara yang memiliki kapasitas teknis tetapi kehilangan kepercayaan publik akan kesulitan mengelola krisis sosial-politik.

Untuk memperjelas perbedaan antara kondisi saat ini dan model yang ditawarkan, artikel ini merumuskan peta reformasi dalam empat tingkat. Tingkat pertama adalah tingkat normatif, yaitu harmonisasi peraturan dan penyusunan payung hukum. Tingkat kedua adalah tingkat kelembagaan, yaitu penguatan koordinasi lintas aktor dan pembagian kewenangan. Tingkat ketiga adalah tingkat operasional, yaitu penyusunan protokol krisis, sistem berbagi informasi, latihan bersama, dan pemulihan. Tingkat keempat adalah tingkat demokratis, yaitu pengawasan, audit, perlindungan hak, dan evaluasi publik. Keempat tingkat tersebut harus berjalan bersama. Pembaruan normatif tanpa kapasitas operasional akan lemah. Koordinasi tanpa akuntabilitas akan berisiko. Akuntabilitas tanpa kapasitas akan membuat negara tidak efektif. Karena itu, reformasi harus bersifat sistemik.

Kontribusi teoretis artikel ini adalah memperluas penggunaan konsep regulatory lag ke dalam kajian keamanan nasional Indonesia. Selama ini regulatory lag lebih sering digunakan dalam pembahasan teknologi, keuangan, dan inovasi digital. Artikel ini menunjukkan bahwa konsep tersebut juga relevan untuk membaca ketertinggalan arsitektur hukum keamanan nasional ketika ancaman berubah menjadi multidomain. Konsep ini membantu menjelaskan bahwa masalah Indonesia bukan hanya belum adanya aturan, melainkan belum sinkronnya regulasi, kelembagaan, definisi ancaman, dan mekanisme koordinasi. Dengan demikian,

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

regulatory lag menjadi lensa untuk membaca hubungan antara perubahan ancaman dan reformasi negara.

Kontribusi praktis artikel ini adalah menawarkan model reformasi yang dapat digunakan pembuat kebijakan. Model Keamanan Nasional Adaptif-Integratif-Demokratis memberi panduan agar reformasi tidak hanya berorientasi pada penambahan kewenangan, tetapi juga pada kejelasan peran, koordinasi lintas lembaga, resiliensi, evaluasi, dan akuntabilitas. Model ini relevan bagi pemerintah, DPR, DPN, BSSN, Kementerian Pertahanan, Polri, TNI, Komdigi, Bappenas, pemerintah daerah, dan aktor nonnegara yang mengelola infrastruktur strategis. Model ini juga mengingatkan bahwa reformasi keamanan nasional harus menjaga warisan positif Reformasi, terutama supremasi sipil dan negara hukum.

Dengan demikian, hasil penelitian ini menegaskan bahwa Indonesia berada pada titik penting. Di satu sisi, negara menghadapi ancaman yang semakin kompleks dan membutuhkan koordinasi lebih kuat. Di sisi lain, pengalaman historis mengajarkan bahwa penguatan keamanan tidak boleh mengorbankan demokrasi. Regulatory lag harus diatasi, tetapi cara mengatasinya harus tepat. Reformasi yang hanya menambah kewenangan tanpa akuntabilitas akan menimbulkan risiko baru. Sebaliknya, reformasi yang hanya menekankan pembatasan tanpa memperkuat kapasitas akan membuat negara rentan. Jalan tengah yang diperlukan adalah reformasi regulasi yang adaptif, integratif, dan demokratis.

Secara lebih konkret, model adaptif-integratif-demokratis dapat diterapkan melalui skema tiga lapis. Lapis pertama adalah lapis pencegahan, yang mencakup pemetaan risiko, standar keamanan minimum, audit kelembagaan, dan pendidikan literasi keamanan digital. Lapis kedua adalah lapis respons, yang mencakup aktivasi protokol krisis, pembagian peran antarlembaga, komunikasi publik, dukungan teknis, dan pemulihan layanan. Lapis ketiga adalah lapis pembelajaran, yang mencakup evaluasi pascakrisis, pembaruan regulasi, sanksi atau koreksi kelembagaan, serta peningkatan kapasitas. Tiga lapis ini penting karena keamanan nasional tidak cukup dibangun melalui dokumen hukum; ia harus hidup dalam praktik kelembagaan yang terlatih dan dapat dievaluasi.

Model ini juga memerlukan indikator kinerja. Beberapa indikator yang dapat digunakan ialah waktu respons terhadap insiden, jumlah latihan krisis lintas sektor, tingkat kepatuhan pelaporan insiden, keberadaan standar resiliensi pada sektor vital, kejelasan pembagian peran, penurunan waktu pemulihan layanan, kualitas komunikasi publik, dan hasil audit independen. Indikator demokratis juga diperlukan, misalnya keberadaan mekanisme pengaduan, perlindungan data warga, evaluasi hak asasi manusia, dan keterbukaan informasi kebijakan secara proporsional. Dengan indikator tersebut, reformasi regulasi dapat diukur sebagai proses tata kelola, bukan hanya sebagai keberhasilan menerbitkan peraturan baru.

Salah satu implikasi penting dari analisis ini adalah perlunya memperluas makna keamanan nasional tanpa kehilangan batasnya. Keamanan nasional memang harus mampu menjangkau ancaman siber, ekonomi, data, energi, dan infrastruktur. Namun, perluasan makna tersebut tidak boleh membuat semua persoalan sosial berubah menjadi isu keamanan. Masalah administrasi, kritik publik, konflik politik normal, atau perbedaan pendapat warga tidak boleh disekuritisasi kecuali memenuhi kriteria ancaman yang jelas, berdampak luas, dan memiliki dasar hukum. Prinsip ini penting agar reformasi keamanan nasional tetap menjaga ruang demokrasi dan tidak menimbulkan ketakutan warga terhadap negara.

Dengan demikian, pembaruan regulasi keamanan nasional harus disertai perubahan budaya birokrasi. Budaya kerja sektoral, saling menunggu, dan tertutup perlu diganti dengan budaya berbagi informasi, koordinasi berbasis risiko, pembelajaran pascakrisis, dan

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

akuntabilitas. Perubahan budaya ini tidak dapat dihasilkan oleh regulasi saja, tetapi regulasi dapat menyediakan insentif dan kewajiban. Misalnya, kewajiban latihan krisis, kewajiban pelaporan insiden, kewajiban audit resiliensi, dan kewajiban evaluasi pascakejadian akan mendorong lembaga bekerja lebih terbuka dan terukur. Oleh karena itu, hukum harus dirancang sebagai instrumen yang mengubah perilaku kelembagaan.

Dari sisi perencanaan pembangunan, agenda keamanan nasional perlu dihubungkan dengan penganggaran dan indikator kinerja lintas sektor. Regulasi yang baik tidak akan efektif apabila kementerian/lembaga tidak memiliki sumber daya, sistem informasi, dan kapasitas manusia untuk melaksanakannya. Oleh karena itu, reformasi regulasi harus dipadukan dengan rencana penguatan kapasitas nasional, termasuk pengembangan talenta siber, standardisasi keamanan sistem elektronik pemerintah, modernisasi infrastruktur data, dan dukungan anggaran untuk latihan krisis. Tanpa dukungan perencanaan dan anggaran, reformasi hukum akan menjadi dokumen normatif yang tidak mengubah praktik.

Sektor privat juga harus ditempatkan sebagai bagian dari ekosistem keamanan nasional kontemporer. Banyak infrastruktur digital, layanan keuangan, logistik, komunikasi, energi, kesehatan, dan platform data dikelola oleh badan usaha atau bekerja melalui kemitraan pemerintah-swasta. Karena itu, regulasi keamanan nasional tidak bisa hanya mengatur aktor negara. Negara perlu menetapkan standar, kewajiban pelaporan, perlindungan data, dan mekanisme kerja sama dengan sektor privat, tetapi juga harus menyediakan insentif dan kepastian hukum. Keterlibatan sektor privat menjadi penting karena krisis multidomain sering kali bergerak melalui jaringan yang tidak sepenuhnya berada di bawah kendali langsung pemerintah.

Pada saat yang sama, masyarakat sipil dan akademisi perlu dilibatkan dalam evaluasi kebijakan. Pelibatan ini bukan untuk membuka rahasia negara, melainkan untuk memastikan bahwa reformasi keamanan nasional tetap sah, proporsional, dan dipercaya publik. Akademisi dapat membantu melakukan kajian risiko dan evaluasi regulasi, sedangkan masyarakat sipil dapat memberi masukan mengenai dampak kebijakan terhadap hak warga. Dengan demikian, reformasi keamanan nasional dapat memperoleh legitimasi sosial, bukan hanya legitimasi formal. Legitimasi ini penting karena keamanan nasional pada akhirnya bergantung pada kerja sama antara negara dan masyarakat.

Selain itu, reformasi perlu menempatkan komunikasi publik sebagai bagian dari manajemen keamanan nasional. Dalam krisis siber atau infrastruktur, ketidakjelasan informasi dapat memperbesar kepanikan, spekulasi, dan disinformasi. Oleh karena itu, protokol krisis harus mengatur siapa juru bicara, informasi apa yang dapat disampaikan, kapan pembaruan diberikan, dan bagaimana negara menjelaskan langkah pemulihan secara jujur tanpa membuka kerentanan teknis yang sensitif.

Rumusannya perlu diuji melalui simulasi periodik nasional.

Tabel 4. Peta Jalan Reformasi Regulasi Keamanan Nasional

Tahap	Fokus	Keluaran Kebijakan
Jangka pendek	Pemetaan regulasi dan protokol koordinasi krisis.	Audit regulasi, peta aktor, protokol respons insiden siber dan infrastruktur kritis.
Jangka menengah	Harmonisasi regulasi dan penguatan kelembagaan.	RUU keamanan dan ketahanan siber, standar resiliensi infrastruktur kritis, latihan bersama nasional.
Jangka panjang	Arsitektur keamanan nasional adaptif dan demokratis.	Regulatory review berkala, pusat pembelajaran krisis nasional, integrasi data risiko lintas sektor.

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

Sumber: Diolah penulis (2026).

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Artikel ini menyimpulkan bahwa keamanan nasional Indonesia menghadapi regulatory lag yang bersifat arsitektural. Ketertinggalan tersebut tidak berarti Indonesia tidak memiliki regulasi, melainkan menunjukkan bahwa regulasi yang ada masih tersebar secara sektoral dan belum bekerja sebagai satu sistem keamanan nasional yang terintegrasi. UU Polri, UU Pertahanan Negara, UU TNI, UU Pelindungan Data Pribadi, Perpres Pelindungan Infrastruktur Informasi Vital, Perpres Strategi Keamanan Siber Nasional, Perpres DPN, RPJMN 2025-2029, dan perubahan UU TNI masing-masing memiliki fungsi penting. Namun, hubungan antarinstrumen tersebut belum cukup kuat untuk menghadapi ancaman multidomain yang bergerak melalui siber, data, infrastruktur kritis, geoekonomi, rantai pasok, energi, informasi, dan stabilitas sosial-politik.

Bentuk regulatory lag paling jelas terlihat pada lima hal. Pertama, terdapat ketidaksesuaian antara definisi ancaman dalam regulasi sektoral dan karakter ancaman kontemporer yang lintas domain. Kedua, terdapat fragmentasi kewenangan antara aktor pertahanan, keamanan dalam negeri, siber, data, komunikasi digital, infrastruktur, dan pemerintah daerah. Ketiga, mekanisme koordinasi lintas kementerian/lembaga belum sepenuhnya operasional dalam menghadapi krisis multidomain. Keempat, integrasi antara keamanan siber, pelindungan data, dan infrastruktur kritis belum ditempatkan secara utuh dalam kerangka keamanan nasional. Kelima, belum terdapat mekanisme evaluasi regulasi berkala yang memungkinkan hukum diperbarui secara adaptif mengikuti perkembangan teknologi dan ancaman.

Political will negara sebenarnya mulai terlihat. Pembentukan Dewan Pertahanan Nasional menunjukkan adanya kesadaran untuk memperkuat forum pertimbangan dan solusi kebijakan pertahanan nasional strategis. Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber menunjukkan pengakuan bahwa siber telah menjadi domain strategis. Pelindungan Infrastruktur Informasi Vital menunjukkan perhatian terhadap aset digital yang penting bagi keberlangsungan layanan negara dan masyarakat. RPJMN 2025-2029 menempatkan keamanan dan ketahanan siber sebagai agenda pembangunan nasional. Perubahan UU TNI juga menunjukkan adanya pembaruan sebagian norma pertahanan. Namun, political will tersebut masih bersifat parsial karena belum terkonsolidasi dalam satu peta jalan reformasi regulasi keamanan nasional yang integratif dan demokratis.

Atas dasar itu, artikel ini menawarkan Model Keamanan Nasional Adaptif-Integratif-Demokratis. Model ini terdiri atas lima komponen: integrasi normatif, koordinasi strategis lintas lembaga, tata kelola risiko dan resiliensi, akuntabilitas demokratis, dan evaluasi adaptif. Integrasi normatif diperlukan untuk menyelaraskan regulasi pertahanan, keamanan dalam negeri, siber, data, infrastruktur kritis, dan ketahanan nasional. Koordinasi strategis diperlukan agar ancaman multidomain tidak terjebak dalam sekat birokrasi. Tata kelola risiko dan resiliensi diperlukan agar negara tidak hanya reaktif, tetapi mampu mencegah, mendeteksi, merespons, memulihkan, dan belajar dari krisis. Akuntabilitas demokratis diperlukan agar penguatan keamanan tidak berubah menjadi sekuritisasi represif. Evaluasi adaptif diperlukan agar regulasi tidak kembali tertinggal dari perkembangan ancaman.

Reformasi regulasi keamanan nasional Indonesia harus membedakan integrasi dari sentralisasi. Integrasi berarti menghubungkan aktor, kewenangan, data, prosedur, dan standar

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com
ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

agar respons negara lebih koheren. Sentralisasi yang berlebihan justru dapat memperbesar risiko penyalahgunaan kewenangan dan melemahkan pengawasan demokratis. Oleh karena itu, pembaruan regulasi harus tetap berpijak pada supremasi sipil, prinsip negara hukum, perlindungan hak warga negara, pengawasan DPR, audit independen, transparansi proporsional, dan mekanisme pengaduan publik. Keamanan nasional yang kuat tidak boleh dibangun dengan mengorbankan demokrasi, karena demokrasi dan kepercayaan publik merupakan bagian dari resiliensi nasional.

Dengan demikian, regulatory lag keamanan nasional Indonesia perlu dipahami sebagai momentum reformasi. Tantangan utama bukan hanya memperbarui satu atau dua regulasi, tetapi membangun arsitektur tata kelola keamanan nasional yang mampu menjawab ancaman abad ke-21. Reformasi tersebut harus membuat negara lebih cepat, lebih terkoordinasi, lebih tangguh, dan lebih akuntabel. Jika pembaruan dilakukan secara parsial, Indonesia akan terus berada dalam posisi reaktif terhadap ancaman. Namun, jika pembaruan dilakukan secara adaptif, integratif, dan demokratis, Indonesia dapat membangun tata kelola keamanan nasional yang sejalan dengan perkembangan ancaman kontemporer sekaligus tetap setia pada prinsip Reformasi, supremasi sipil, dan negara hukum.

5.2 Saran

Secara praktis, pemerintah dan DPR perlu menyusun peta jalan reformasi regulasi keamanan nasional. Peta jalan tersebut dapat mencakup harmonisasi definisi ancaman, penguatan payung hukum keamanan dan ketahanan siber, pengaturan perlindungan infrastruktur kritis secara lebih komprehensif, penyusunan protokol nasional respons krisis multidomain, dan regulatory review setiap tiga sampai lima tahun. DPN dapat dikembangkan sebagai simpul pertimbangan strategis di bidang pertahanan nasional, tetapi penguatan perannya perlu disertai kejelasan mandat, hubungan kerja, dan batas kewenangan. BSSN, Polri, TNI, Komdigi, kementerian teknis, pemerintah daerah, sektor privat, dan masyarakat sipil perlu ditempatkan dalam ekosistem koordinasi yang jelas.

Akhirnya, penelitian ini memiliki keterbatasan karena menggunakan pendekatan normatif-preskriptif dan belum menguji implementasi regulasi melalui wawancara, survei, atau studi kasus empiris mendalam. Penelitian berikutnya dapat menguji model ini pada kasus konkret, misalnya serangan siber terhadap layanan publik, krisis infrastruktur digital, gangguan rantai pasok strategis, atau koordinasi lintas lembaga dalam manajemen krisis. Penelitian empiris juga dapat menilai apakah aktor-aktor negara memiliki persepsi yang sama mengenai ancaman multidomain dan apakah mekanisme koordinasi yang tersedia sudah bekerja. Meskipun demikian, artikel ini memberikan dasar konseptual dan normatif untuk membaca regulatory lag sebagai persoalan mendesak dalam reformasi keamanan nasional Indonesia.

Karena itu, rekomendasi utama artikel ini adalah agar pembaruan regulasi keamanan nasional dilakukan melalui pendekatan bertahap, terukur, dan partisipatif. Pemerintah perlu memulai dari audit regulasi, pemetaan kewenangan, dan penyusunan protokol krisis. Tahap berikutnya adalah harmonisasi regulasi siber, data, dan infrastruktur kritis. Tahap akhir adalah pembentukan mekanisme evaluasi adaptif yang memastikan regulasi selalu diperbarui sesuai perkembangan ancaman dan tetap berada dalam koridor demokrasi.

DAFTAR PUSTAKA

Ahern, D. (2021). Regulatory lag, regulatory friction and regulatory transition as FinTech disenablers: Calibrating an EU response to the regulatory sandbox phenomenon. *European Business Organization Law Review, 22*, 395–432. https://doi.org/10.1007/s40804-021-00217-z

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

Aji, M. P. (2025). Cybersecurity politics in building cyber sovereignty in Indonesia through strengthening the role of the National Cyber and Crypto Agency. *Society, 13*(2), 1056–1071. https://doi.org/10.33019/society.v13i2.960

Ananta, A. R. R., Wicaksono, D. B., Indrawati, I., Istikhomah, I., & Amalina, Z. (2025). Potensi konflik kewenangan pada perlindungan dari ancaman siber di Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 14*(2), 233–252. https://doi.org/10.33331/rechtsvinding.v14i2.2199

Aryanti, D. R. (2025). Cybersecurity governance in public institutions: Managing digital risks and resilience. *VISIONER: Jurnal Pemerintahan Daerah di Indonesia, 17*(3), 24–35. https://doi.org/10.54783/jv.v17i3.1424

Atkins, S., & Lawson, C. (2021). An improvised patchwork: Success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review, 81*(5), 847–861. https://doi.org/10.1111/puar.13322

Badan Pembinaan Hukum Nasional. (2024). *Laporan akhir kelompok kerja analisis dan evaluasi hukum pertahanan negara*. Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia. https://bphn.go.id/data/documents/laporan_akhir_pokja_ae_pertahanan_negara_2024_final.pdf

Badan Pembinaan Hukum Nasional. (2025, April 30). *Pertajam hasil analisis dan evaluasi terkait keamanan siber, Pusanev gelar rapat narasumber dengan BSSN*. https://bphn.go.id/berita-utama/pertajam-hasil-analisis-dan-evaluasi-terkait-keamanan-siber-pusanev-gelar-rapat-narasumber-dengan-bssn

Baldwin, D. A. (1995). Security studies and the end of the Cold War. *World Politics, 48*(1), 117–141. https://doi.org/10.1353/wp.1995.0001

Bappenas. (2025). *Rencana Pembangunan Jangka Menengah Nasional 2025–2029*. Kementerian PPN/Bappenas.

Booth, K. (Ed.). (2005). *Critical security studies and world politics*. Lynne Rienner Publishers.

Buzan, B. (1991). *People, states and fear: An agenda for international security studies in the post-Cold War era* (2nd ed.). Lynne Rienner Publishers.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press. https://doi.org/10.1017/CBO9780511817762

Collins, A. (Ed.). (2025). *Contemporary security studies* (7th ed.). Oxford University Press.

Djuyandi, Y., Dewi, S. K., Rahayu, L. F., & Hassan, M. S. (2025). Civil-military relations in Indonesia: Promoting a professional military character from the New Order era to the Reform era. *Otoritas: Jurnal Ilmu Pemerintahan, 15*(3), 510–530. https://doi.org/10.26618/ojip.v15i3.18714

Fajar, H. F., Fadhila, A., & Yades, M. K. (2025). Redesain kebijakan hukum keamanan dan ketahanan siber: Studi kasus serangan siber pada Pusat Data Nasional tahun 2024. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 14*(2). https://doi.org/10.33331/rechtsvinding.v14i2.2155

Hipdizah, H., Purwanto, S., Hendarwoto, Y., Duarte, R., Siagian, F., & Anggraeni, D. (2025). Buku ajar doktrin militer. *YPAD Penerbit*.

Indonesia. (2002a). *Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia*.

Indonesia. (2002b). *Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara*.

Indonesia. (2004). *Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia*.

Indonesia. (2022a). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*.

Indonesia. (2022b). *Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital*.

Indonesia. (2023). *Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber*.

Indonesia. (2024). *Peraturan Presiden Nomor 202 Tahun 2024 tentang Dewan Pertahanan Nasional*.

Indonesia. (2025a). *Peraturan Presiden Nomor 12 Tahun 2025 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2025–2029*.

Indonesia. (2025b). *Undang-Undang Nomor 3 Tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia*.

International Monetary Fund. (2025). *World economic outlook update, July 2025: Global economy: Tenuous resilience amid persistent uncertainty*. https://doi.org/10.5089/9798229017305.081

SPARTA
MULTIDISCIPLINARY JOURNAL
https://jurnal.patriotbangsapublisher.com/smj
Email: admin@jurnal.patriotbangsapublisher.com

ISSN XXXX – XXXX
VOL 1, NO 1
MEI 2026

Mardes, S., Putra, Y., Purwanto, S., Putri, R. D., & Ramadhani, E. (2026). Cultural beliefs and mental health: Exploring Ethiopia's spiritual and societal pathways. *Explore (New York, NY)*, *22*(3), 103346-103346.

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors, 22*(2), 538. https://doi.org/10.3390/s22020538

Purwanto, S., Supangat, S., Esterina, M., Souhoka, S., Chandra, F., Hariputra, A., ... & Arianto, T. (2024). *Manajemen sumber daya manusia*. Yayasan Tri Edukasi Ilmiah.

Purwanto, S., Purnomo, M. R., & Budiman, H. (2025). Power Dynamics in Decision Making: A Qualitative Analysis. *Power*, *2*(1), 80-86.

Purwanto, S., & Ismail, D. E. (2024). Manajemen Risiko. *Kalimantan Selatan: Ruang Karya*.

Purwanto, S., Hidayatullah, S. S. W., & Tirtoadisuryo, D. (2025). Human resource development strategies for enhancing organizational performance In the digital era. *International Journal of Financial Economics*, *1*(7), 662-668.

Purwanto, S., & Siagian, F. (2025). Strategic human resources management in the global era: Navigating opportunities and challenges. *Centurion MSPD Journal*, *1*(1), 1-13.

SIPRI. (2026). *Trends in world military expenditure, 2025*. Stockholm International Peace Research Institute. https://www.sipri.org/publications/2026/sipri-fact-sheets/trends-world-military-expenditure-2025

Stojanović-Gajić, S., & Pavlović, D. (2021). State capture, hybrid regimes, and security sector reform. *Journal of Regional Security, 16*(2), 89–126. https://doi.org/10.5937/jrs0-34622

Tagarev, T., & Fluri, P. (2025). From civil-military relations to resilience: The fifth wave of strengthening democracy through research and education. *Connections: The Quarterly Journal, 24*(1), 73–90. https://doi.org/10.11610/Connections.24.1.06

Taş, H. (2024). Populism and civil-military relations. *Democratization, 31*(1), 70–89. https://doi.org/10.1080/13510347.2023.2255976

Tomaževič, N., Kovač, P., Ravšelj, D., Umek, L., Babaoğlu, C., Bohatá, M., Hirsch, B., Kulaç, O., Nurlybaeva, G. K., Schäfer, F.-S., & Aristovnik, A. (2023). The role of agile values in enhancing good governance in public administration during the COVID-19 crisis: An international survey. *Administrative Sciences, 13*(12), 248. https://doi.org/10.3390/admsci13120248

Walt, S. M. (1991). The renaissance of security studies. *International Studies Quarterly, 35*(2), 211–239. https://doi.org/10.2307/2600471

Williams, P. D., & McDonald, M. (Eds.). (2023). *Security studies: An introduction* (4th ed.). Routledge. https://doi.org/10.4324/9781003247821

World Economic Forum. (2026). *The global risks report 2026* (21st ed.). https://www.weforum.org/publications/global-risks-report-2026/