



Rekonstruksi Doktrin Sishankamrata di Era Digital: Model Berjenjang Ambang untuk Adaptasi terhadap Ancaman Siber Asimetris

Reconstructing the Sishankamrata Doctrine in the Digital Era: A Threshold-Graduated Model for Adapting to Asymmetric Cyber Threats

Yogi Sugama Takasita Manik^{1*}, Fatmil Dwi Pambudi², Lukman Hakim³

^{1,2,3}Fakultas Strategi Pertahanan, Universitas Pertahanan Republik Indonesia

*email penulis koresponden: yogidamanik@gmail.com

Abstrak. Doktrin Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) bertumpu pada logika mobilisasi yang biner, yaitu damai atau perang, sedangkan ancaman siber asimetris di zona abu-abu berlangsung terus-menerus di bawah ambang perang. Lumpuhnya Pusat Data Nasional Sementara 2 (PDNS 2) pada Juni 2024 memperlihatkan jarak antara doktrin, tata kelola, dan kelembagaan. Penelitian ini bertujuan merekonstruksi Sishankamrata untuk domain siber melalui tinjauan naratif kritis atas literatur nasional dan internasional, analisis teks hukum, kasus ilustratif PDNS 2, serta perbandingan terstruktur-terfokus dengan empat model pertahanan semesta (Nordik, Singapura, Estonia, dan Ukraina). Hasil telaah menunjukkan bahwa *doctrinal lag* bukan sekadar kesenjangan antara domain fisik dan digital, melainkan ketidaksesuaian antara logika mobilisasi biner dan karakter persaingan siber yang berkelanjutan. *Governance mismatch* muncul karena mode tata kelola jejaring yang dipakai tidak sesuai dengan kontingensinya, sedangkan *structural void* terletak pada ketiadaan penghubung operasional berbasis undang-undang. Kebaruan artikel ini adalah Model Sishankamrata Siber Berjenjang Ambang (SSBA), yang memetakan empat ambang ancaman terhadap jalur hukum pelibatan talenta sipil, mode tata kelola, peran TNI, dan mekanisme kontrol sipil, dengan pemicu transisi yang tercatat dan dapat diturunkan kembali. Dalam jangka dekat, jalur Komponen Pendukung dan pengabdian sesuai profesi lebih layak daripada Komponen Cadangan, yang terhalang ketiadaan matra siber dan syarat mobilisasi. Model ini dilengkapi peta jalan bergerbang dengan 13 indikator dan tiga proposisi yang dapat diuji secara empiris.

Kata kunci: Sishankamrata; *total defence*; ancaman siber asimetris; zona abu-abu; tata kelola jejaring; ambang eskalasi; kontrol sipil

Abstract. The Total People's Defense and Security System (Sishankamrata) doctrine rests on a binary mobilization logic of peace or war, whereas asymmetric cyber threats in the gray zone unfold continuously below the threshold of war. The paralysis of Temporary National Data Center 2 (PDNS 2) in June 2024 exposed a gap between doctrine, governance, and institutions. This study reconstructs Sishankamrata for the cyber domain through a critical narrative review of national and international literature, legal text analysis, the illustrative PDNS 2 case, and a structured, focused comparison with four total defence models (the Nordic states, Singapore, Estonia, and Ukraine). The review shows that doctrinal lag is not merely a gap between physical and digital domains but a mismatch between binary

mobilization and the continuous character of cyber competition. Governance mismatch arises because the network governance mode in use does not fit its contingencies, while the structural void lies in the absence of a statute-based operational link. The article's novelty is the Threshold-Graduated Cyber Sishankamrata (SSBA) model, which maps four threat thresholds onto legal pathways for civilian talent, governance modes, the role of the armed forces, and civilian control mechanisms, with recorded and reversible transition triggers. In the near term, the Supporting Component and profession-based service are more feasible than the Reserve Component, which is constrained by the absence of a cyber branch and by mobilization requirements. The model is accompanied by a gated roadmap with 13 indicators and three empirically testable propositions.

Keywords: Sishankamrata; total defence; asymmetric cyber threats; gray zone; network governance; escalation thresholds; civilian control

1. Pendahuluan

1.1 Latar Belakang

Ancaman keamanan nasional kini banyak bergerak di ruang yang tidak melintasi perbatasan fisik. Operasi zona abu-abu (*gray zone*) dan serangan siber asimetris memanfaatkan kerentanan infrastruktur digital, celah regulasi, dan ketimpangan kapabilitas untuk menimbulkan kelumpuhan strategis tanpa konfrontasi militer terbuka (Novrianto et al., 2026). Literatur strategi internasional menjelaskan bahwa ruang siber mengaburkan batas antara perang dan damai serta antara ranah publik dan privat (Kello, 2013). Persaingan di ruang ini berlangsung sebagai kampanye berkelanjutan di bawah ambang serangan bersenjata, yang dampak strategisnya terbentuk secara kumulatif, bukan melalui satu pukulan yang menentukan (Harknett & Smeets, 2022). Aktor eksternal juga dapat memanfaatkan keterbukaan masyarakat demokratis melalui gangguan hibrida yang sengaja dibuat ambigu agar tidak memicu respons militer (Wigell, 2019). Ancaman ini tidak menggantikan kekuatan militer konvensional, tetapi menambah domain yang harus dipertahankan dan menuntut bentuk pertahanan yang berbeda.

Indonesia telah merasakan dampaknya. Pada 20 Juni 2024, Pusat Data Nasional Sementara 2 (PDNS 2) di Surabaya dilumpuhkan *ransomware Brain Cipher* yang berbasis *LockBit 3.0*. Serangan itu mengganggu sekitar 282 instansi atau layanan

pemerintah, termasuk layanan imigrasi di Bandara Soekarno-Hatta (detikINET, 2024; Puspita D. et al., 2025; Saputra et al., 2026). Tekanan pada ruang siber nasional juga tinggi: BSSN mencatat 3,64 miliar anomali lalu lintas siber pada Januari–Juli 2025 (Nurhakim, 2025).

Sishankamrata, sebagaimana diatur dalam UU No. 3 Tahun 2002 tentang Pertahanan Negara, dirancang terutama untuk menghimpun potensi nasional di domain fisik. Literatur menilai bahwa ruang siber belum tertata terpadu dalam kerangka itu (Novrianto et al., 2026), sedangkan regulasi keamanan siber masih tersebar dan tumpang tindih (Al Asyari, 2023). Negara-negara lain yang menganut konsep pertahanan semesta justru telah memperbarui doktrinnya. Negara-negara Nordik menghidupkan kembali *total defence* sebagai pendekatan seluruh masyarakat untuk membangun ketahanan sejak masa damai (Wither, 2020; Wrange et al., 2024), dan Singapura menambahkan *Digital Defence* sebagai pilar keenam *Total Defence* pada 2019 (MCI & MINDEF, 2019). Pada tingkat tata kelola, Indonesia telah menerbitkan Perpres No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber serta UU No. 3 Tahun 2025 tentang perubahan UU TNI. Namun, tata kelola tetap terfragmentasi karena BSSN yang hanya berlandaskan Perpres tidak memiliki daya paksa terhadap lembaga yang dibentuk dengan undang-undang (Pamungkas et al., 2026).

1.2 Celah Penelitian dan Kebaruan

Kajian terdahulu tentang Indonesia mengelompok pada sekuritisasi dan strategi pertahanan siber (Permana, 2021; Wibowo et al., 2024), sinergi antarlembaga (Rizki & Timur, 2021; Suhirwan, 2026), kelembagaan angkatan siber (Adma et al., 2023; Suwandi et al., 2026), pembiayaan pertahanan (Marsudiyanto, 2025; Matthews et al., 2025), serta kesadaran dan peran masyarakat (Ginting et al., 2025). Kajian terdekat adalah Novrianto et al. (2026), yang mengidentifikasi tiga persoalan, yaitu *doctrine lag*, *governance mismatch*, dan *structural void*, memperkenalkan istilah *administrative lag*, serta merekomendasikan *Total Civic Resilience*, korps cadangan siber-ekonomi, dan

Dewan Keamanan Nasional (DKN) sebagai pusat komando operasional. Di tingkat internasional, literatur *total defence* (Wither, 2020; Wrange et al., 2024) dan perdebatan tentang sifat persaingan siber (Rid, 2012; Kello, 2013; Maschmeyer, 2021; Harknett & Smeets, 2022) berkembang pesat, tetapi belum dihubungkan dengan doktrin Sishankamrata dan kerangka hukum tiga komponen pertahanan Indonesia.

Artikel ini tidak mengklaim tiga persoalan tersebut sebagai temuannya sendiri. Kebaruannya terletak pada tiga kontribusi. **Pertama, kontribusi teoretis:** artikel ini merumuskan ulang *doctrinal lag* sebagai ketidaksesuaian antara logika mobilisasi Sishankamrata yang biner dan episodik dengan karakter persaingan siber yang berkelanjutan dan berjenjang, bukan sekadar kesenjangan domain fisik dan digital. **Kedua, kontribusi konseptual:** artikel ini mengajukan Model Sishankamrata Siber Berjenjang Ambang (SSBA), yang memetakan empat ambang ancaman terhadap jalur hukum pelibatan sipil menurut UU No. 23 Tahun 2019, mode tata kelola jejaring menurut teori kontingensi Provan dan Kenis (2008), peran TNI, status hukum peserta sipil, dan mekanisme kontrol sipil. **Ketiga, kontribusi komparatif dan metodologis:** artikel ini menempatkan Sishankamrata dalam perbandingan terstruktur dengan empat model pertahanan semesta internasional, memisahkan bukti resmi dan sekunder pada kasus PDNS 2, serta menurunkan peta jalan bergerbang dengan indikator terukur dan proposisi yang dapat diuji.

1.3 Pertanyaan, Tujuan, dan Sistematika

Pertanyaan utama penelitian ini adalah bagaimana doktrin Sishankamrata dapat direkonstruksi untuk menghadapi ancaman siber asimetris dengan tetap memenuhi batas hukum dan kontrol sipil. Tujuannya ada tiga: (1) memetakan kesenjangan doktrin, tata kelola, dan kelembagaan berdasarkan telaah literatur nasional dan internasional; (2) menguji kelayakan hukum, bukti kasus, dan pelajaran komparatif atas usulan rekonstruksi; serta (3) menyintesis model berjenjang ambang dan peta jalan bergerbang yang dapat diukur. Artikel ini terdiri atas lima bagian: pendahuluan, tinjauan pustaka dan landasan teori, metode, hasil dan diskusi, serta kesimpulan.

2. Tinjauan Pustaka

2.1 Penelitian Terdahulu dan Celah

Literatur yang relevan dapat dikelompokkan dalam sembilan arus, tujuh tentang pertahanan siber Indonesia (2021–2026) dan dua dari literatur internasional. Ringkasannya disajikan pada Tabel 1.

Tabel 1. Ringkasan Penelitian Terdahulu dan Keterbatasannya

Arus kajian	Penulis (tahun)	Temuan yang relevan	Keterbatasan terhadap penelitian ini
Sekuritisasi dan strategi	Wibowo et al. (2024); Permana (2021)	Unit siber Kemhan dibentuk dengan peraturan menteri sehingga kewenangannya terbatas pada Kemhan dan TNI; strategi mitigasi mencakup pencegahan, identifikasi, dan pemulihan	Belum dikaitkan dengan doktrin Sishankamrata dan komponen sipil
Sinergi antarlembaga	Rizki & Timur (2021); Suhirwan (2026)	Enam pemangku kepentingan dengan BSSN sebagai <i>leading sector</i> ; hambatan klasifikasi dan notifikasi lintas lembaga pada kasus maritim	Rizki & Timur bersifat normatif; Suhirwan berkonteks maritim dan berbasis wawancara
Hukum dan kewenangan	Pamungkas et al. (2026); Syahril et al. (2026)	BSSN tanpa daya paksa terhadap TNI dan Polri; tiada protokol eskalasi; pembagian tanggung jawab lembaga pada insiden PDNS	Kajian hukum; tidak membahas pembiayaan dan talenta sipil
Manajemen pertahanan	Novrianto et al. (2026)	Tiga persoalan, <i>administrative lag</i> , <i>Total Civic Resilience</i> , DKN sebagai pusat komando	Esai tinjauan kritis; belum menguji kelayakan hukum, perbandingan, dan peta jalan
Angkatan siber	Adma et al. (2023); Suwandi et al. (2026)	Jalur BSSN-dulu versus Komando Gabungan TNI-dulu; tiga fase	Jeda antartahap tanpa alasan; tanpa indikator gerbang
Fiskal pertahanan	Marsudiyanto (2025); Matthews et al. (2025); Bachtiar et al. (2026)	Kesenjangan fiskal; ketergantungan pinjaman luar negeri; kepekaan belanja pertahanan terhadap inflasi dan kurs	Tidak khusus pertahanan siber
Kebebasan sipil	Alzaki et al. (2026); Al Asyari (2023)	Risiko <i>over-securitization</i> ; kebutuhan UU keamanan siber dengan partisipasi publik	Tidak membahas peta jalan
Teori persaingan siber (internasional)	Rid (2012); Kello (2013); Maschmeyer (2021); Harknett & Smeets (2022)	Operasi siber umumnya berupa subversi, spionase, dan sabotase di bawah ambang perang; efek strategis bersifat kumulatif	Berbasis pengalaman negara besar; tidak membahas doktrin pertahanan semesta negara berkembang

Arus kajian	Penulis (tahun)	Temuan yang relevan	Keterbatasan terhadap penelitian ini
<i>Total defence</i> dan relawan siber (internasional)	Wither (2020); Wrange et al. (2024); Kaska et al. (2013); Done (2023)	Kebangkitan pertahanan seluruh masyarakat; unit relawan siber dengan dasar hukum khusus; risiko hukum relawan ofensif	Tidak dikaitkan dengan kerangka tiga komponen UU No. 23/2019

Sumber: telaah penulis (2026).

Dari ringkasan itu tampak empat celah. Pertama, celah hukum-doktrinal: belum ada uji kelayakan hukum atas gagasan pelibatan talenta digital sipil dalam kerangka UU No. 23/2019, padahal usulan korps cadangan siber sudah beredar (Novrianto et al., 2026). Kedua, celah bukti empiris: klaim tentang kelumpuhan PDNS 2 bertumpu pada sumber sekunder yang kualitas dan konsistensinya beragam. Ketiga, celah kelembagaan: peta jalan angkatan siber (Adma et al., 2023; Suwandi et al., 2026) belum menjelaskan alasan jeda antartahap maupun indikator yang menentukan kapan tahap berikutnya boleh dimulai. Keempat, celah teoretis-komparatif: Sishankamrata belum diposisikan dalam literatur *total defence* internasional dan perdebatan tentang sifat persaingan siber, sehingga rekomendasi kebijakan cenderung meminjam istilah tanpa menguji kesesuaiannya dengan karakter ancaman.

2.2 Landasan Teori

Penelitian ini memakai tiga tingkat teori sebagai alat analitis. Tingkat umum (*grand theory*) adalah *security governance*, yang menjelaskan pergeseran dari struktur keamanan terpusat ke struktur yang lebih terfragmentasi dengan peran aktor swasta dan nonpemerintah (Krahmann, 2003). Dalam keamanan siber, fragmentasi itu diperkuat oleh kompleksitas teknologi dan sebaran kepemilikan infrastruktur, sehingga politik keamanan siber bersifat berjejaring (Dunn Cavelty & Wenger, 2020). Teori ini dipakai untuk memahami mengapa pertahanan siber tidak dapat bertumpu pada satu institusi militer.

Tingkat menengah (*middle-range theory*) menghubungkan konsep umum dengan konteks Indonesia melalui tiga konsep. Pertama, Sishankamrata dipahami sebagai varian doktrin pertahanan semesta yang menghimpun Komponen Utama, Komponen

Cadangan, dan Komponen Pendukung (UU No. 3/2002; UU No. 23/2019). Literatur *total defence* menunjukkan bahwa doktrin semacam ini relevan bagi ancaman kontemporer bila ketahanan masyarakat dibangun sejak masa damai, bukan hanya disiapkan untuk mobilisasi masa perang (Wither, 2020). Kedua, tata kelola jejaring (*network governance*) memandang jejaring sebagai bentuk tata kelola utama sambil mempertimbangkan sisi demokratisnya (Sørensen & Torfing, 2007). Provan dan Kenis (2008) membedakan tiga mode, yaitu jejaring yang diatur partisipan, organisasi pemimpin (*lead organization*), dan organisasi administratif jejaring (*network administrative organization*, NAO). Efektivitas setiap mode bergantung pada empat kontingensi: tingkat kepercayaan, jumlah partisipan, konsensus tujuan, dan kebutuhan kompetensi pada tingkat jejaring. Dari sana penelitian ini memakai istilah operasional *networked defense governance*, yaitu koordinasi lintas lembaga sipil, militer, dan swasta dengan pembagian peran yang jelas, pertukaran informasi ancaman yang cepat, dan kewenangan keputusan yang ditetapkan hukum di bawah kontrol sipil. Ketiga, kontrol sipil dipahami dalam pengertian kontrol sipil objektif (Huntington, 1957) yang diperluas oleh Croissant et al. (2010) ke lima arena keputusan: rekrutmen elite, kebijakan publik, keamanan dalam negeri, pertahanan nasional, dan organisasi militer.

Tingkat operasional memakai tiga perangkat. Pertama, *administrative lag*, istilah yang diperkenalkan Novrianto et al. (2026) untuk keterlambatan respons birokrasi akibat koordinasi berjenjang. Penelitian ini mendefinisikannya secara operasional sebagai selang waktu antara deteksi anomali dan keputusan respons lintas lembaga. Kedua, perdebatan tentang sifat persaingan siber. Satu kubu menekankan bahwa operasi siber berlangsung sebagai keterlibatan terus-menerus di bawah ambang perang (Healey, 2019; Harknett & Smeets, 2022). Kubu lain mengingatkan bahwa operasi siber umumnya berupa subversi dengan efek strategis terbatas (Rid, 2012; Maschmeyer, 2021) dan nyaris tidak memengaruhi peristiwa di medan tempur (Kostyuk & Zhukov, 2019). Kedua kubu sama-sama menyiratkan bahwa ancaman

siber utama bagi negara seperti Indonesia adalah gangguan berkelanjutan di bawah ambang perang, bukan "perang siber" yang dinyatakan. Ketiga, konsep perang asimetris Buffaloe (2006), yang memuat empat aspek: ancaman asimetris, operasi asimetris, asimetri budaya, dan biaya asimetris. Aspek ini dilengkapi teori interaksi strategis Arreguín-Toft (2001), yang menunjukkan bahwa hasil konflik asimetris ditentukan oleh kecocokan pendekatan strategis kedua pihak, bukan semata oleh besarnya kekuatan. Keempat aspek Buffaloe adalah aspek konseptual, bukan variabel dalam persamaan yang dapat dihitung. Pemetaannya pada tiga persoalan disajikan pada Tabel 2.

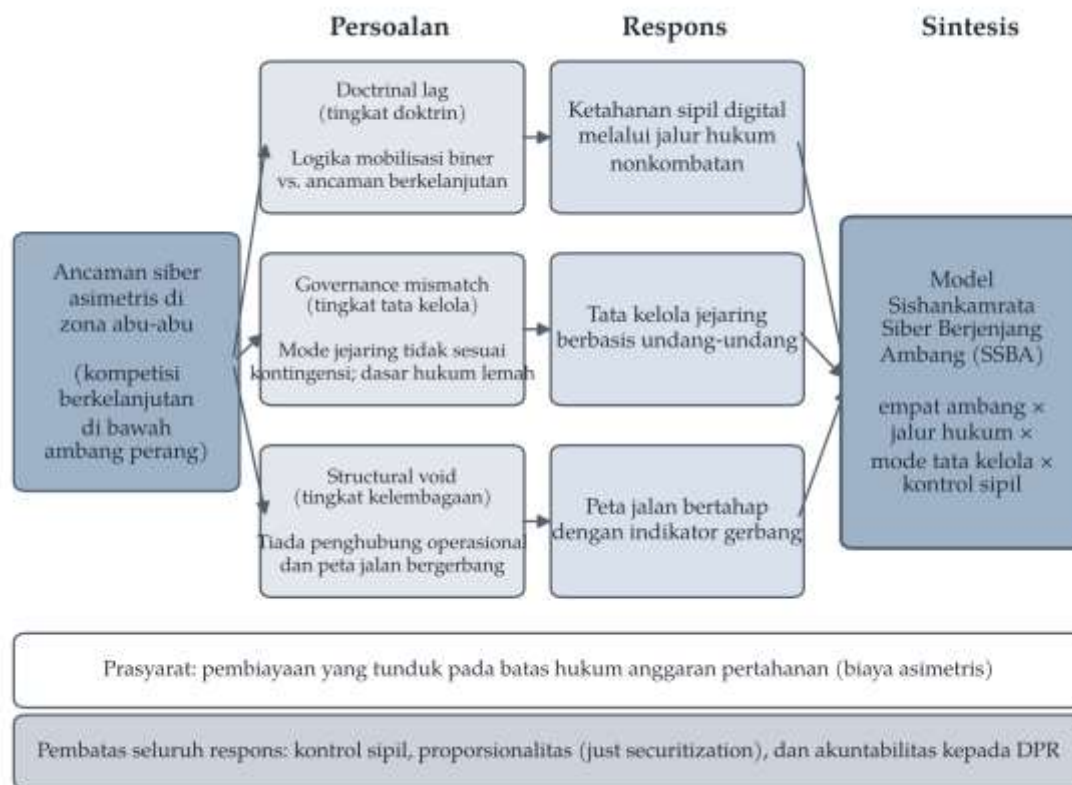
Tabel 2. Pemetaan Aspek Buffaloe (2006) terhadap Tiga Persoalan

Aspek Buffaloe	Makna	Persoalan terkait	Pemakaian dalam analisis
Ancaman asimetris	Pihak lemah menyerang kelemahan pihak kuat	Latar seluruh persoalan	Menjelaskan ancaman siber dan zona abu-abu
Operasi asimetris	Cara pihak yang diserang beroperasi dan merespons	<i>Governance mismatch; structural void</i>	Menganalisis koordinasi, mode tata kelola, dan struktur komando
Asimetri budaya	Perbedaan nilai dan peran penduduk	<i>Doctrinal lag</i>	Menganalisis peran warga dan talenta sipil
Biaya asimetris	Ketimpangan biaya penyerang dan pembela	Prasyarat fiskal	Menganalisis pembiayaan dan kemitraan

Sumber: Buffaloe (2006); pemetaan merupakan tafsiran penulis.

2.3 Kerangka Konseptual

Kerangka konseptual penelitian ini disajikan pada Gambar 1. Ancaman siber asimetris di zona abu-abu menekan sistem pertahanan sebagai persaingan berkelanjutan di bawah ambang perang. Tekanan itu tampak dalam tiga persoalan, yaitu *doctrinal lag* pada tingkat doktrin, *governance mismatch* pada tingkat tata kelola, dan *structural void* pada tingkat kelembagaan. Setiap persoalan dijawab dengan respons yang sesuai, yaitu ketahanan sipil digital melalui jalur hukum nonkombatan, tata kelola jejaring berbasis undang-undang, dan peta jalan kapabilitas bergerbang. Ketiga respons disintesis menjadi Model SSBA. Pembiayaan menjadi prasyarat pelaksanaan, dan seluruh respons dibatasi oleh kontrol sipil, proporsionalitas, dan akuntabilitas.



Gambar 1. Kerangka Konseptual Rekonstruksi Sishankamrata untuk Domain Siber

Sumber: disusun penulis (2026).

3. Metode Penelitian

3.1 Desain Penelitian

Penelitian ini adalah tinjauan naratif kritis (*critical narrative review*) dengan pendekatan kualitatif. Dalam tipologi Grant dan Booth (2009), tinjauan kritis tidak sekadar meringkas, tetapi mengevaluasi literatur dan menghasilkan sintesis berupa kerangka konseptual yang bersifat hipotetis. Pendekatan ini dipilih karena tujuannya menilai, membandingkan, dan menyintesis gagasan, kerangka hukum, dan kebijakan tentang adaptasi Sishankamrata, bukan menghitung efek. Penelitian ini tidak mengklaim sebagai *systematic literature review* dan tidak mengikuti protokol PRISMA 2020. Transparansi pelaporan mengacu pada kriteria SANRA (Baethge et al., 2019). Tinjauan ini dilengkapi perbandingan terstruktur-terfokus (*structured, focused comparison*) (George & Bennett, 2005) terhadap empat model pertahanan semesta internasional. Berbeda dari Novrianto et al. (2026), penelitian ini menambahkan

analisis pasal, verifikasi bukti kasus pada dokumen primer, dan perbandingan internasional.

3.2 Pertanyaan Penelitian

Tiga pertanyaan turunan memandu penelitian ini. RQ1: bagaimana literatur nasional dan internasional menjelaskan kesenjangan antara Sishankamrata dan karakter ancaman siber, dan bagaimana kelayakan hukum jalur pelibatan talenta sipil? RQ2: faktor tata kelola apa yang menghambat respons lintas lembaga pada insiden siber nasional? RQ3: bagaimana kelembagaan, pembiayaan, dan kontrol sipil dapat ditata dalam model berjenjang dan peta jalan yang dapat diukur?

3.3 Pencarian dan Pemilihan Sumber

Sumber akademik dicari secara purposif pada 5–10 Oktober 2026 melalui Scopus, Web of Science, Google Scholar, dan Portal Garuda/SINTA dengan kata kunci berbahasa Indonesia dan Inggris, misalnya Sishankamrata, *total defence*, *gray zone*, *cyber defense*, *persistent engagement*, *network governance*, *civilian control*, pertahanan siber, Komponen Cadangan, dan *cyber force*. Pencarian dilengkapi penelusuran bola salju (*snowball*) dari daftar pustaka sumber kunci. Kriteria inklusinya adalah artikel jurnal, prosiding, buku akademik, atau laporan lembaga riset kebijakan yang membahas doktrin, kebijakan, tata kelola, atau pertahanan siber. Untuk kajian tentang Indonesia, rentang terbitnya 2021–2026, sedangkan untuk literatur teori dan perbandingan internasional dipilih karya yang terbit di jurnal bereputasi terindeks Scopus atau Web of Science tanpa batas tahun bila karya itu menjadi rujukan dasar. Opini media tidak dipakai sebagai dasar argumen konseptual. Hasilnya, 49 sumber akademik substantif ditelaah, di luar empat rujukan metodologis. Sumber itu terdiri atas 23 kajian tentang Indonesia, lima di antaranya terbit di jurnal internasional bereputasi, dan 26 karya teoretis serta komparatif internasional. Metadata setiap artikel jurnal dicocokkan dengan Crossref atau laman penerbit. Karena penelusuran bersifat purposif, tidak semua literatur tercakup.

3.4 Data Pendukung

Tiga jenis data pendukung dibedakan dari literatur akademik. Pertama, dokumen hukum, yaitu UU No. 3/2002, UU No. 34/2004, UU No. 23/2019, UU No. 3/2025, UU No. 27/2022, PP No. 71/2019, Perpres No. 28/2021, dan Perpres No. 47/2023, yang dianalisis sebagai teks normatif. Kedua, kasus PDNS 2 (Juni 2024) sebagai kasus ilustratif, dengan fakta kronologis diambil dari keterangan resmi BSSN yang dikutip media dan dibandingkan dengan studi sekunder. Ketiga, dokumen resmi negara perbandingan dan pemberitaan media, yang hanya melengkapi fakta peristiwa dan selalu ditandai sebagai data sekunder.

3.5 Prosedur Analisis

Analisis dilakukan dalam lima langkah. Langkah pertama adalah pembacaan dan pengodean sumber secara deduktif berdasarkan tiga pertanyaan penelitian. Langkah kedua adalah pengelompokan kode menjadi tema mengikuti Braun dan Clarke (2006) dan pemetaan tema ke tiga persoalan. Langkah ketiga adalah evaluasi kritis: setiap tema dibandingkan antarsumber untuk melihat kesepakatan, perbedaan, dan celah, termasuk pandangan yang berlawanan. Langkah keempat adalah perbandingan terstruktur-terfokus. Empat model perbandingan, yaitu Nordik, Singapura, Estonia, dan Ukraina, diajukan lima pertanyaan seragam: dasar hukum pelibatan sipil, status sipil atau militer peserta, pemimpin koordinasi masa damai, pemicu eskalasi, dan mekanisme akuntabilitas. Keempat model dipilih karena mewakili variasi yang bermakna, mulai dari pertahanan semesta yang dilembagakan, pilar digital berbasis sipil, unit relawan berdasar hukum khusus, hingga mobilisasi relawan secara ad hoc. Langkah kelima adalah penurunan model dan peta jalan dengan jalur penalaran yang eksplisit dari temuan ke implikasi doktrinal, tata kelola, kelembagaan, dan fiskal. Untuk menjaga mutu, klaim empiris penting dirujuk ke sumber primer, bukti dikelompokkan menurut tingkat keandalannya (Tabel 5), dan pernyataan umum seperti "mayoritas studi" hanya dipakai bila disertai jumlah.

3.6 Keterbatasan

Penelusuran bersifat purposif dan tidak mencakup penilaian kualitas formal setiap sumber. Sebagian sumber berasal dari 2025–2026 dan belum banyak disitasi. Kasus PDNS 2 hanyalah satu kasus, sehingga temuan tidak dapat digeneralisasi. Perbandingan internasional bertumpu pada sumber sekunder, bukan studi lapangan. Model yang diajukan bersifat hipotetis dan memerlukan pengujian melalui studi kasus, wawancara pemangku kepentingan, simulasi biaya, atau teknik Delphi.

4. Hasil dan Diskusi

4.1 *Doctrinal Lag*: Dari Mobilisasi Biner ke Ketahanan Sipil Berjenjang

Telaah memperlihatkan bahwa UU No. 23/2019 sudah mengakui serangan siber sebagai wujud ancaman dan membedakan ancaman militer, nonmiliter, dan hibrida (UU No. 23/2019, Pasal 4). Karena itu, *doctrinal lag* tidak terletak pada pengakuan hukum. Persoalannya ada pada logika mobilisasi. Sishankamrata menyiapkan sumber daya nasional pada masa damai untuk dikerahkan ketika keadaan berubah menjadi darurat militer atau perang (UU No. 23/2019, Pasal 63). Logika ini biner dan episodik, sedangkan persaingan siber berlangsung terus-menerus dan berjenjang di bawah ambang perang (Kello, 2013; Harknett & Smeets, 2022). Akibatnya, sebagian besar ancaman siber nyata, seperti serangan *ransomware* terhadap PDNS 2, tidak pernah memenuhi syarat untuk memicu perangkat Sishankamrata. Novrianto et al. (2026) mencatat bahwa sebagian besar anggaran modernisasi pertahanan dalam lima tahun terakhir mengalir ke alat utama sistem senjata dan komponen cadangan yang dirancang untuk perlawanan fisik. Al Asyari (2023) menambahkan bahwa regulasi keamanan siber masih tersebar di banyak undang-undang dan lembaga yang tumpang tindih.

Rumusan ulang ini juga menuntut kehati-hatian terhadap militerisasi. Bila operasi siber umumnya bersifat subversif dengan dampak strategis terbatas (Rid, 2012; Maschmeyer, 2021), respons yang paling relevan adalah ketahanan, deteksi, dan

pemulihan di ranah sipil, bukan perluasan peran militer. Penelitian ini mengadopsi gagasan *Total Civic Resilience* dari Novrianto et al. (2026), yang menafsirkan pertahanan rakyat bukan sebagai militerisasi warga, melainkan ketahanan sipil, termasuk literasi digital dan pelibatan peretas, ilmuwan data, dan analis ekonomi. Definisi operasional yang dipakai di sini adalah kemampuan unsur bangsa, yaitu pemerintah, warga berkompetensi digital, dan pelaku usaha, untuk mendeteksi, menahan, dan memulihkan diri dari serangan siber terhadap fungsi vital negara melalui jalur yang diatur hukum dan di bawah kontrol sipil. Literatur kritis mengingatkan bahwa wacana ketahanan dapat menggeser tanggung jawab dari negara ke individu dan masyarakat (Dunn Cavelty et al., 2015). Karena itu, ketahanan sipil dalam artikel ini tidak mengurangi kewajiban hukum negara dan penyelenggara sistem elektronik. Dalam kerangka Buffaloe (2006), gagasan ini bersangkut dengan asimetri budaya, yaitu peran penduduk dalam konflik asimetris. Ginting et al. (2025) menegaskan perlunya literasi digital dan kolaborasi pemerintah, swasta, dan masyarakat, tetapi tidak merinci mekanisme hukumnya.

Kelayakan hukum pelibatan talenta sipil berbeda antarjalur (Tabel 3). Jalur Komponen Cadangan, yang diusulkan Novrianto et al. (2026) dan Pamungkas et al. (2026), menghadapi hambatan yang besar. UU No. 23/2019 hanya mengelompokkan Komponen Cadangan menurut matra darat, laut, dan udara (Pasal 31), menyiapkannya untuk ancaman militer dan hibrida (Pasal 29), mensyaratkan usia 18–35 tahun dan pelatihan dasar kemiliteran tiga bulan (Pasal 33 dan 35), menerapkan hukum militer pada masa aktif (Pasal 46), dan hanya membolehkan mobilisasi pada keadaan darurat militer atau perang dengan persetujuan DPR (Pasal 63). Dengan demikian, mobilisasi Komponen Cadangan untuk krisis siber masa damai seperti PDNS 2 tidak sesuai dengan ketentuan yang berlaku. Persyaratan itu juga bertolak belakang dengan praktik cadangan siber di negara lain, yang justru melonggarkan syarat kebugaran, usia, dan kesiapan penugasan agar profesional sipil berpengalaman dapat bergabung (Brill & Fairtlough, 2020). Jalur Komponen

Pendukung dan pengabdian sesuai profesi lebih layak dalam jangka dekat karena bersifat sukarela, nonkombatan, dan dapat dikoordinasikan kementerian atau lembaga terkait.

Tabel 3. Jalur Hukum Pelibatan Talenta Digital Sipil menurut UU No. 23/2019

Jalur	Dasar pasal	Kelebihan	Hambatan
A. Komponen Pendukung (tenaga ahli, warga terlatih, dan sarana siber)	Pasal 17–20, termasuk Pasal 20 ayat (1) dan ayat (3) huruf d	Sukarela; dapat dipakai langsung atau tidak langsung menghadapi ancaman militer dan hibrida; bersifat nonkombatan saat mobilisasi (Pasal 65 ayat (2))	Pengaturan dan pembinaan melalui peraturan pemerintah (Pasal 24 dan 27) perlu dicek apakah sudah mencakup siber
B. Pengabdian sesuai profesi	Pasal 6 ayat (2) huruf d; Pasal 15 ayat (4)	Untuk ancaman nonmiliter yang dikoordinasikan kementerian/lembaga terkait, sehingga cocok bagi peran BSSN dan Kemkomdigi	Perlu peraturan pelaksana yang jelas (Pasal 16)
C. Komponen Cadangan siber	Pasal 28–31	Terstruktur di bawah Komponen Utama	Tidak ada matra siber (Pasal 31); disiapkan untuk ancaman militer dan hibrida (Pasal 29); usia 18–35 tahun (Pasal 33); pelatihan dasar kemiliteran tiga bulan (Pasal 35); hukum militer pada masa aktif (Pasal 46); mobilisasi hanya pada darurat militer atau perang dengan persetujuan DPR (Pasal 63)

Sumber: UU No. 23 Tahun 2019; analisis penulis.

Perbandingan internasional memperjelas pilihan tersebut (Tabel 4). Model Nordik menunjukkan bahwa pertahanan semesta dapat diperbarui menjadi kesiapsiagaan seluruh masyarakat pada masa damai, dengan peran sektor swasta yang diatur sejak awal (Wither, 2020; Wrange et al., 2024). Singapura memisahkan pilar *Digital Defence*, yang menekankan peran warga sebagai pengguna yang aman, waspada, dan bertanggung jawab, dari kapabilitas siber militer (Adma et al., 2023; MCI & MINDEF, 2019). Estonia melibatkan relawan siber melalui unit khusus dalam Liga Pertahanan dengan dasar hukum dan seleksi yang dirancang tersendiri (Kaska et al., 2013). Sebaliknya, *IT Army* Ukraina merekrut relawan secara terbuka untuk operasi ofensif. Model ini efektif secara taktis, tetapi status hukum pesertanya kabur (Done, 2023). Menurut hukum humaniter internasional, warga sipil kehilangan

perlindungan dari serangan selama mereka berpartisipasi langsung dalam permusuhan, termasuk melalui operasi siber (Schmitt, 2017, Rule 97). Pelajaran bagi Indonesia jelas: pelibatan talenta sipil perlu diberi dasar hukum khusus, dibatasi pada fungsi defensif dan pemulihan, dan tidak dibiarkan terbentuk secara ad hoc.

Tabel 4. Perbandingan Terstruktur Model Pertahanan Semesta dalam Domain Siber

Pertanyaan	Nordik (Finlandia, Swedia)	Singapura	Estonia	Ukraina	Indonesia (kondisi saat ini)
Dasar hukum pelibatan sipil	Kerangka <i>total defence</i> dan keamanan menyeluruh	Pilar <i>Digital Defence</i> dalam <i>Total Defence</i>	Unit siber Liga Pertahanan dengan dasar hukum khusus	Ad hoc; dibentuk kementerian digital saat perang	UU No. 23/2019; tanpa matra atau jalur siber khusus
Status peserta	Sipil; sektor swasta terlibat sejak masa damai	Warga sipil; kapabilitas militer terpisah (DIS)	Relawan dalam organisasi pertahanan	Relawan sipil dalam dan luar negeri	Komcad (militer saat aktif) atau Komponen Pendukung (nonkombatan)
Pemimpin koordinasi masa damai	Otoritas sipil dengan perencanaan bersama	Kementerian sipil dan pertahanan bersama	Organisasi pertahanan dengan dukungan pada otoritas sipil	Tidak jelas	BSSN berbasis Perpres; tanpa daya paksa
Pemicu eskalasi	Bertingkat menurut tingkat kesiapsiagaan	Kampanye berkelanjutan masa damai	Krisis atau perang	Perang	Biner: darurat militer atau perang
Akuntabilitas	Parlemen dan pengawasan sipil	Pemerintah sipil	Rantai komando dan hukum nasional	Kabur; risiko partisipasi langsung dalam permusuhan	DPR (Pasal 76 UU No. 23/2019)
Pelajaran	Bangun ketahanan sejak damai	Pisahkan peran warga dari kapabilitas militer	Relawan butuh dasar hukum khusus	Hindari relawan ofensif	Perlu jenjang ambang dan jalur defensif

Sumber: Wither (2020); Wrange et al. (2024); MCI & MINDEF (2019); Adma et al. (2023); Kaska et al. (2013); Done (2023); Schmitt (2017); UU No. 23 Tahun 2019; analisis penulis.

Pelibatan sipil membawa risiko. UU No. 23/2019 sendiri mensyaratkan pengelolaan yang demokratis dan menghormati hak asasi manusia serta pengawasan oleh komisi DPR bidang pertahanan (Pasal 19 ayat (2), Pasal 30 ayat (2), dan Pasal 76). Pamungkas et al. (2026) mengusulkan perlindungan hukum bagi talenta sipil yang dimobilisasi untuk tindakan aktif, termasuk serangan balik yang dalam keadaan biasa dapat dipidana menurut UU ITE. Usulan itu perlu dibahas dengan hati-hati. Selain

bertabrakan dengan prinsip proporsionalitas dan akuntabilitas yang ditekankan kerangka *just securitization* (Floyd, 2011; Alzaki et al., 2026), serangan balik oleh warga sipil dapat menjadikan mereka sasaran sah bila terjadi konflik bersenjata (Schmitt, 2017). Hansen dan Nissenbaum (2009) juga mengingatkan bahwa wacana keamanan siber mudah mengalami hipersekuritisasi karena skenario bencana digital sulit dibantah publik. *Total Civic Resilience* karena itu perlu menekankan kesukarelaan, batas peran nonkombatan dan defensif, serta pengawasan, agar tidak dibaca sebagai perluasan militerisasi ruang siber.

4.2 Governance Mismatch dan Administrative Lag: Pelajaran dari PDNS 2

Kasus PDNS 2 dipakai sebagai kasus ilustratif. Menurut BSSN, upaya menonaktifkan Windows Defender terdeteksi sejak 17 Juni 2024 pukul 23.15 WIB, aktivitas berbahaya dimulai 20 Juni pukul 00.54 WIB, dan pertahanan lokal gagal pada pukul 00.55 WIB (Cloudcomputing.id, 2024; detikINET, 2024). Studi sekunder melaporkan sekitar 282 instansi atau layanan terdampak serta cadangan data yang tidak memadai (Puspita D. et al., 2025; Saputra et al., 2026), tetapi sebagian angka kronologinya belum dapat diverifikasi pada dokumen resmi (Tabel 5). Karena sumber resmi tidak menyebut kapan lembaga-lembaga terkait mengambil keputusan, *administrative lag* kasus ini tidak dapat dihitung secara kuantitatif. Selang 49 jam 39 menit antara menonaktifkan Windows Defender dan dimulainya aktivitas berbahaya adalah selang aktivitas penyerang, bukan *administrative lag*.

Tabel 5. Kronologi dan Tingkat Bukti Kasus PDNS 2 (Juni 2024)

Waktu	Fakta	Tingkat bukti dan sumber	Implikasi analitis
17 Juni 2024, 23.15 WIB	BSSN menemukan upaya menonaktifkan Windows Defender yang memungkinkan aktivitas berbahaya berjalan	A. Keterangan BSSN yang dikutip media (Cloudcomputing.id, 2024; detikINET, 2024)	Titik awal keberhasilan penyerang pada lapis pertahanan titik akhir
20 Juni 2024, 00.54 WIB	Aktivitas berbahaya dimulai, termasuk penghapusan <i>filesystem</i> penting dan menonaktifkan komponen penyimpanan	A. Laporan forensik sementara BSSN yang dikutip media (detikINET, 2024)	Sasaran lapis penyimpanan memperkecil peluang pemulihan

Waktu	Fakta	Tingkat bukti dan sumber	Implikasi analitis
20 Juni 2024, 00.55 WIB	Windows Defender gagal beroperasi	A. BSSN (Cloudcomputing.id, 2024; detikINET, 2024)	Pertahanan lokal gagal dalam satu menit
20 Juni 2024	Layanan imigrasi Bandara Soekarno-Hatta terganggu	A/B. Media dan studi sekunder (Cloudcomputing.id, 2024; Puspita D. et al., 2025)	Dampak pada layanan publik strategis
20 Juni 2024	Sekitar 282 instansi atau layanan lumpuh	B. Puspita D. et al. (2025) menulis "instansi"; Saputra et al. (2026) menulis "layanan"	Satuan hitung belum seragam; perlu rilis resmi
20 Juni 2024, 00.30 dan 08.15 WIB	Deteksi anomali dan konfirmasi serangan	B. Saputra et al. (2026), berbasis wawancara; bertentangan dengan BSSN (aktivitas mulai 00.54)	Tidak dipakai sebagai dasar keterlambatan
Pemulihan	Pemulihan penuh dilaporkan 15 Agustus 2024	B. Saputra et al. (2026), satu sumber	Perlu sumber resmi
Cadangan data	"Hanya 30" server (Saputra et al.) dan "hanya 2 data" (Puspita D. et al.) memiliki cadangan	B. Dua sumber saling bertentangan	Ditulis kualitatif: cadangan tidak memadai

Keterangan: A = pernyataan resmi lembaga yang dikutip media; B = studi akademik sekunder. Sumber: analisis penulis.

Meskipun demikian, literatur menunjukkan tiga manifestasi *governance mismatch*. Pertama, fragmentasi dasar hukum dan kewenangan. BSSN yang berlandaskan Perpres bertanggung jawab sebagai koordinator, tetapi tidak memiliki daya paksa terhadap TNI dan Polri, dan tidak ada protokol eskalasi dari ranah sipil ke pertahanan (Pamungkas et al., 2026). Syahrial et al. (2026) menambahkan bahwa pada PDNS berlaku tanggung jawab bersama, dengan instansi pengguna bertanggung jawab atas sistem dan cadangan datanya, sedangkan kewajiban pencadangan belum ditetapkan pemilik layanan. Pandangan berbeda datang dari Adma et al. (2023), yang menilai Perpres No. 47/2023 sudah cukup sebagai payung hukum sementara sambil menunggu RUU keamanan siber.

Kedua, perbedaan klasifikasi informasi. Suhirwan (2026) melaporkan satu contoh dari insiden *ransomware* pelabuhan Batam 2023, ketika BSSN mengklasifikasikan ancaman sebagai "*Confidential*" sedangkan BAKAMLA mensyaratkan "*Secret*" untuk peringatan maritim, berdasarkan satu informan wawancara. Contoh ini berkonteks maritim dan karena itu dipakai sebagai analogi, bukan bukti kasus PDNS. Ketiga,

pemrosesan berurutan. Novrianto et al. (2026) menggambarkan rantai koordinasi berjenjang yang berjalan dalam hitungan hari bahkan pekan, sedangkan Saputra et al. (2026) melaporkan, berdasarkan wawancara, bahwa satuan tugas gabungan baru efektif pada hari keempat. Kedua sumber ini kualitasnya terbatas dan perlu dikonfirmasi dengan dokumen resmi.

Teori kontingensi Provan dan Kenis (2008) membantu menjelaskan mengapa ketiga manifestasi itu muncul. Ekosistem keamanan siber nasional melibatkan ratusan instansi dan penyelenggara sistem elektronik, kepercayaan antarlembaga rendah (tampak dari perbedaan klasifikasi), konsensus tujuan baru sebagian, dan kebutuhan kompetensi pada tingkat jejaring tinggi. Kepercayaan yang rendah sebenarnya cocok dengan mode organisasi pemimpin, tetapi jumlah partisipan yang besar dan kebutuhan kompetensi yang tinggi lebih cocok dengan NAO. Dalam praktik, Indonesia memakai mode organisasi pemimpin, tetapi organisasi pemimpinnya, yaitu BSSN, tidak memiliki dasar hukum setingkat undang-undang. Inilah inti *governance mismatch*: mode yang dipilih tidak didukung oleh kewenangan yang dibutuhkannya. Pengalaman Indonesia di domain maritim memperlihatkan pola serupa. Arif et al. (2024) menunjukkan bahwa ambiguitas taktik zona abu-abu berbenturan dengan upaya reformasi tata kelola keamanan maritim Indonesia yang menuntut pembagian tegas antara lembaga sipil dan angkatan laut. Pembagian peran yang kaku tanpa mekanisme transisi justru mengurangi kelenturan respons.

Untuk menjawab persoalan itu, penelitian ini mengusulkan *networked defense governance* dengan tiga prinsip. Pembagian peran: BSSN memimpin perlindungan siber sipil, sedangkan TNI menjalankan operasi militer selain perang (OMSP) pertahanan siber terhadap ancaman bernuansa militer sebagaimana dimandatkan UU No. 3/2025 (Suwandi et al., 2026). Pertukaran informasi: protokol klasifikasi bersama dan serah terima kewenangan dari penegakan hukum ke pertahanan, yang oleh Rizki dan Timur (2021) dipetakan menurut eskalasi ancaman, kejahatan, dan perang siber. Keputusan terpadu: satu mekanisme koordinasi krisis lintas kementerian/lembaga

dengan kewenangan yang ditetapkan undang-undang. Novrianto et al. (2026) mengusulkan DKN untuk peran ini. Karena status hukum DKN belum diuraikan dalam sumber yang ditelaah dan kewenangan komando yang luas menimbulkan kekhawatiran kontrol sipil (Croissant et al., 2010), penelitian ini memperlakukan DKN sebagai salah satu opsi kelembagaan, bukan satu-satunya.

4.3 Efisiensi Pembiayaan sebagai Prasyarat

Pertahanan siber menuntut investasi besar di tengah ruang fiskal yang sempit. Belanja pertahanan Indonesia berkisar 0,6–0,7% PDB, dan sekitar 85% pengadaan proyek dibiayai pinjaman luar negeri (Matthews et al., 2025). Kebutuhan Renstra 2020–2024 hanya terpenuhi sekitar 33% oleh anggaran negara (Matthews et al., 2025). Marsudiyanto (2025) memperkirakan celah fiskal pertahanan berlanjut hingga 2045 bila hanya mengandalkan pertumbuhan pendapatan negara sekitar 1,5% per tahun. Angka celah tahunan dalam artikel itu tidak konsisten, sehingga hanya dipakai sebagai gambaran umum. Bachtiar et al. (2026) menunjukkan bahwa belanja pertahanan peka terhadap inflasi dan kurs, dan menyarankan obligasi pertahanan serta kemitraan publik-swasta sebagai pembiayaan jangka panjang. Dalam kerangka Buffaloe (2006), ini adalah aspek biaya asimetris: penyerang bermodal rendah, sedangkan pembela menanggung biaya lapis demi lapis.

Tabel 6. Skema Pembiayaan, Dasar, dan Batasannya

Skema	Dasar dan sumber	Batasan atau risiko
A. Kewajiban penyelenggara sistem elektronik menanggung keamanan sistemnya, disertai insentif	UU ITE Pasal 15 mewajibkan penyelenggara sistem menyelenggarakan sistem secara andal dan aman; pada PDNS berlaku tanggung jawab bersama (Syahrial et al., 2026). Insentif berupa dana riset atau keringanan pajak (Nurtrihadi et al., 2025)	Insentif memerlukan dasar hukum tersendiri
B. Pelibatan talenta sipil melalui Komponen Pendukung atau pengabdian sesuai profesi (Tabel 3)	Biaya dasar berupa pelatihan, perangkat, dan tunjangan; peserta tetap bekerja di instansi asal	Biaya Komponen Cadangan (pelatihan dasar kemiliteran, hukum militer) belum dihitung; perlu simulasi biaya

Skema	Dasar dan sumber	Batasan atau risiko
C. Sumber lain yang sah dan kemandirian kriptografi	Perpres No. 47/2023 Pasal 34 huruf c dan Pasal 11; mandat R&D dan alih teknologi pada BUMN industri pertahanan (Achmadi et al., 2025); mandat kemandirian kriptografi yang menurut Syahril et al. (2026) belum dijalankan BSSN	Pendanaan TNI harus bersumber dari anggaran negara (Matthews et al., 2025); utang Defend ID di atas Rp15 triliun dan R&D di bawah 1% pendapatan (Achmadi et al., 2025)

Sumber: analisis penulis berdasarkan sumber yang dikutip.

Skema A tidak disebut *co-financing* sukarela, karena dasarnya adalah kewajiban hukum penyelenggara sistem elektronik. Pilihan ini sejalan dengan temuan Carr (2016) bahwa kemitraan publik-swasta dalam strategi keamanan siber nasional sering gagal karena pihak swasta enggan memikul tanggung jawab keamanan nasional, sehingga akuntabilitas menjadi kabur. Di Indonesia, Saputra et al. (2019) menemukan bahwa kemitraan publik-swasta di bidang keamanan siber terhambat oleh rendahnya penerimaan sektor swasta dan ketidakjelasan pembagian risiko, sehingga memerlukan kerangka hukum yang mengikat. Skema B tidak mengklaim bahwa Komponen Cadangan siber menghindari belanja pegawai, karena biaya pelatihan dasar kemiliteran dan hukum militer belum dihitung. Skema C memanfaatkan "sumber lain yang sah" tanpa mengklaim bahwa PNBP atau CSR disebut eksplisit dalam Perpres No. 47/2023. Satu batas hukum penting adalah bahwa pendanaan TNI wajib bersumber dari anggaran negara (UU No. 3/2002 Pasal 25; UU No. 34/2004 Pasal 66), sehingga dana swasta harus disalurkan melalui kementerian, BSSN, atau BUMN, bukan langsung ke TNI (Matthews et al., 2025).

Pembiayaan berbasis kemitraan membawa risiko. Marsudiyanto (2025) mencatat bahwa keterlibatan swasta dapat mengurangi kendali negara atas aset pertahanan, dan penerbitan obligasi dapat menambah beban fiskal bila hasilnya tidak sesuai harapan. Kajian historis yang melibatkan penulis yang sama menemukan bahwa usulan seperti kemitraan publik-swasta jarang terlaksana karena kompromi politik dan inefisiensi struktural (Marsudiyanto et al., 2025). Achmadi et al. (2025) mengakui risiko beban fiskal berlebih dari mandat yang kaku dan menawarkan kemitraan serta

co-financing sebagai mitigasi. Karena itu, skema A–C diajukan sebagai opsi yang perlu diuji kelayakannya.

4.4 Mengisi *Structural Void*: Koordinasi Terpadu dan Peta Jalan Bergerbang

Literatur menunjukkan bahwa persoalan Indonesia bukan ketiadaan lembaga, melainkan ketiadaan penghubung operasional yang berdasar hukum kuat. Novrianto et al. (2026) menemukan tiadanya kerangka komando permanen yang dapat memerintah kementerian sipil dan militer sekaligus pada krisis nonperang. Pamungkas et al. (2026) menunjukkan bahwa tidak ada protokol eskalasi dari ranah sipil ke pertahanan. Wibowo et al. (2024) mencatat bahwa unit siber Kemhan dibentuk dengan peraturan menteri, tidak berstatus organisasi struktural, dan tidak berwenang melindungi lembaga di luar Kemhan dan TNI. Untuk konteks IKN, Reksoprodjo (2026) menyimpulkan bahwa kewenangan komando antara TNI, Polri, BIN, dan OIKN belum jelas.

Dua jalur muncul dalam literatur. Jalur sipil-dulu (Adma et al., 2023) menjadikan BSSN poros jangka pendek dengan unit siber tiap matra sebagai cikal bakal, dan menempatkan angkatan siber sebagai target jangka menengah atau panjang karena hambatan biaya, sumber daya, waktu, dan regulasi. Jalur militer-dulu (Suwandi et al., 2026) memulai dari Komando Gabungan Siber TNI. Narasumber BSSN yang dikutip Suwandi et al. menilai angkatan siber baru diperlukan jika terjadi perang fisik, sedangkan Rektor Unhan mengusulkan komando khusus tingkat Kotama dalam 5–10 tahun sebagai langkah awal. Penelitian ini mengusulkan jalur gabungan sebagai tafsiran penulis: BSSN memimpin perlindungan siber sipil, Komando Gabungan Siber TNI menjalankan mandat OMSP, dan ambang eskalasi di antara keduanya diatur undang-undang (Pamungkas et al., 2026). Jalur gabungan ini menjadi tulang punggung Model SSBA pada subbagian 4.5.

Tabel 7. Peta Jalan Bertahap Kapabilitas Siber Pertahanan

Tahap	Rentang	Isi utama	Sumber
Fase I: Inisiasi dan konsolidasi	Tahun 1–3	Komando Gabungan Siber TNI (menyatukan Satsiber TNI, Pussansiad, Pussiberal, Pusiberau); <i>national cyber range</i> ; <i>national fusion center</i> bersama BSSN dan BIN; paralel dengan penguatan BSSN dan unit siber tiap matra	Suwandi et al. (2026); Adma et al. (2023)
Fase II: Pertahanan aktif	Tahun 3–7	<i>Threat hunting</i> , <i>deception/honeynet</i> , <i>sinkholing</i> ; pelindungan IIVN strategis; kapabilitas serangan balik terbatas hanya oleh Komponen Utama dengan pengawasan hukum dan politik ketat	Suwandi et al. (2026); Schmitt (2017)
Jeda evaluasi	Tahun 7–10	Pemeriksaan indikator gerbang (Tabel 8)	Tafsiran penulis; alasan waktu dan regulasi dari Adma et al. (2023)
Fase III: Matra mandiri	Tahun 10–15	Angkatan Siber sebagai matra keempat, akademi militer siber, satuan regional, selaras dengan Sishankamrata, bila gerbang terpenuhi	Suwandi et al. (2026)

Sumber: Suwandi et al. (2026) dan Adma et al. (2023); penamaan jeda evaluasi merupakan tafsiran penulis.

Rentang tahun 7–10 sudah ada pada Suwandi et al. (2026), tetapi tanpa penjelasan. Durasi total 15 tahun berada dalam kisaran patokan internasional: Singapura membutuhkan sekitar 7 tahun dari pembentukan CSA hingga DIS, dan Tiongkok sekitar 20 tahun dari rencana *information warfare* 1995 hingga *Strategic Support Force* 2015 (Adma et al., 2023). Hambatan talenta nyata: kebutuhan 9 juta talenta digital berbanding kapasitas produksi sekitar 50 ribu per tahun (Adma et al., 2023), yang menurut perhitungan penulis setara 180 tahun bila kekurangan itu ditutup hanya dengan produksi tersebut.

Jeda dirancang sebagai gerbang, bukan penundaan. Tabel 8 merumuskan 13 indikator terukur. Indikator hukum dan kontrol sipil bersifat wajib, sedangkan indikator operasional, anggaran, SDM, dan teknis harus terpenuhi sebagian besar selama dua tahun anggaran berturut-turut. Seluruh ambang adalah usulan awal yang perlu divalidasi, misalnya melalui panel pakar dengan teknik Delphi pada penelitian lanjutan.

Tabel 8. Indikator Gerbang Fase III dan Ambang Usulan

Kode	Indikator terukur	Kondisi dasar (sumber)	Ambang gerbang (usulan penulis)
H1	UU keamanan dan ketahanan siber berlaku dan memuat ambang eskalasi dari ranah sipil ke pertahanan	BSSN hanya berlandaskan Perpres; tiada protokol eskalasi (Pamungkas et al., 2026)	Terpenuhi (ya/tidak); wajib
H2	Revisi UU TNI dan UU Pertahanan Negara memungkinkan matra baru	Pembentukan angkatan siber memerlukan revisi kedua UU (Adma et al., 2023)	Terpenuhi (ya/tidak); wajib
K1	Evaluasi independen atas proporsionalitas dan legitimasi diserahkan ke DPR	Risiko <i>over-securitization</i> (Alzaki et al., 2026)	Satu laporan per tahun; wajib
K2	Partisipasi publik dalam penyusunan regulasi terdokumentasi	RUU keamanan siber perlu melibatkan publik (Al Asyari, 2023)	Terdokumentasi; wajib
O1	Persentase notifikasi ancaman BSSN yang direspons instansi	182 dari 2.200 (sekitar 8,3%) (Adma et al., 2023)	≥ 80%
O2	Median waktu dari deteksi ke pemberitahuan resmi lintas lembaga untuk insiden kritis	Kanal formal regional 48–72 jam dibanding kanal informal di bawah satu jam, konteks maritim (Suhirwan, 2026)	≤ 1 jam
O3	Persentase laporan insiden antarlembaga dalam format terstruktur	Pertukaran masih lewat PDF dan surel; penginputan ulang 6–8 jam, konteks maritim (Suhirwan, 2026)	≥ 90%
O4	Latihan simulasi insiden lintas lembaga dengan laporan evaluasi	Simulasi insiden disarankan untuk menguji koordinasi (Reksoprodjo, 2026)	≥ 1 kali per tahun
A1	Alokasi anggaran BSSN terhadap kebutuhan ideal terverifikasi	Rp700 miliar dari Rp3 triliun, sekitar 23% (Adma et al., 2023)	≥ 80%
A2	Cakupan kebutuhan Renstra pertahanan siber oleh anggaran negara	33% kebutuhan Renstra 2020–2024 pertahanan secara umum (Matthews et al., 2025)	≥ 70%
S1	Persentase formasi unit siber <i>dedicated</i> yang terisi	Sekitar 4–5 operator terampil per divisi dari ideal 20, pernyataan Menhan (Wibowo et al., 2024)	≥ 80%
S2	Pasokan talenta siber terhadap target tahunan nasional	Kebutuhan 9 juta berbanding produksi sekitar 50 ribu per tahun (Adma et al., 2023)	≥ 100% target selama tiga tahun berturut-turut
T1	<i>National cyber range</i> dan <i>fusion center</i> beroperasi	Keluaran Fase I (Suwandi et al., 2026)	Operasional dan teruji

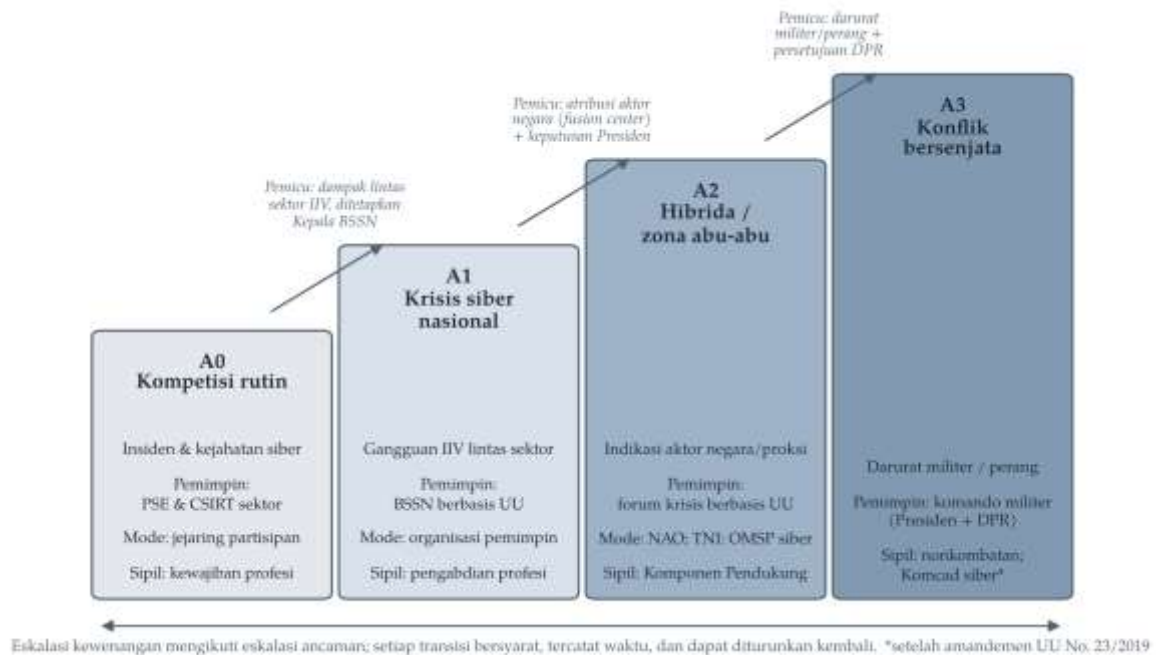
Keterangan: ambang adalah usulan awal penulis dan belum divalidasi. Aturan keputusan: Fase III dimulai bila H1, H2, K1, dan K2 terpenuhi, serta sedikitnya 6 dari 9 indikator lain (O1–O4, A1, A2, S1, S2, T1) terpenuhi selama dua tahun anggaran berturut-turut. Sumber: analisis penulis.

Alasan untuk gerbang kontrol sipil kuat. Alzaki et al. (2026) mengingatkan bahwa sekuritisasi ancaman kognitif berisiko menjadi *over-securitization*, mengikis kebebasan

sipil, dan menjadi permanen lewat tata kelola rutin. Kerangka *just securitization* menilai tindakan luar biasa melalui legitimasi ancaman, proporsionalitas respons, dan perlindungan prinsip demokrasi (Floyd, 2011; Alzaki et al., 2026). Al Asyari (2023) menambahkan bahwa pembahasan RUU keamanan siber harus melibatkan partisipasi publik dan bahwa pengecualian keamanan nasional dalam UU PDP membatasi hak subjek data. Peta jalan ini bersifat konseptual dan bersandar pada satu sumber utama untuk fase-fasenya (Suwandi et al., 2026), yang sendiri merujuk Fitri (2025, sebagaimana dikutip dalam Suwandi et al., 2026), serta belum memuat data biaya atau waktu empiris.

4.5 Sintesis: Model Sishankamrata Siber Berjenjang Ambang (SSBA)

Ketiga persoalan di atas bermuara pada satu masalah desain: kewenangan, jalur pelibatan sipil, dan mekanisme kontrol ditetapkan seolah-olah hanya ada dua keadaan, damai dan perang. Model SSBA menggantikan dikotomi itu dengan empat ambang ancaman (Gambar 2 dan Tabel 9). Ambang A0 adalah kompetisi rutin berupa insiden dan kejahatan siber sehari-hari. Ambang A1 adalah krisis siber nasional, yaitu gangguan infrastruktur informasi vital (IIV) lintas sektor seperti PDNS 2. Ambang A2 adalah ancaman hibrida atau zona abu-abu dengan indikasi keterlibatan aktor negara atau proksinya. Ambang A3 adalah konflik bersenjata atau darurat militer. Pembedaan ambang ini sejalan dengan literatur yang menekankan bahwa strategi hibrida sengaja beroperasi dalam ambiguitas agar tidak memicu respons yang menentukan (Lanoszka, 2016; Wigell, 2019).



Gambar 2. Model Sishankamrata Siber Berjenjang Ambang (SSBA)

Sumber: disusun penulis (2026) berdasarkan UU No. 23/2019, Perpres No. 47/2023, UU No. 3/2025, Provan dan Kenis (2008), dan Schmitt (2017).

Tabel 9. Matriks Model SSBA: Ambang, Kewenangan, Jalur Sipil, dan Kontrol

Dimensi	A0 Kompetisi rutin	A1 Krisis siber nasional	A2 Hibrida/zona abu-abu	A3 Konflik bersenjata
Dasar hukum utama	UU ITE; PP No. 71/2019; UU PDP	Perpres No. 47/2023 (manajemen krisis siber); UU keamanan siber (usulan)	UU No. 23/2019 (ancaman hibrida); UU No. 3/2025 (OMSP siber)	UU No. 3/2002; UU No. 23/2019 Pasal 63
Pemimpin	Penyelenggara sistem elektronik dan CSIRT sektor	BSSN dengan kewenangan setingkat UU	Forum krisis lintas lembaga berbasis UU (DKN atau alternatif)	Komando militer di bawah Presiden
Mode tata kelola (Provan & Kenis, 2008)	Jejaring yang diatur partisipan	Organisasi pemimpin	NAO	Hierarki militer dengan dukungan sipil
Jalur talenta sipil	Kewajiban profesi; pelaporan kerentanan	Pengabdian sesuai profesi (Pasal 6 dan 15)	Komponen Pendukung, defensif dan nonkombatan	Komponen Pendukung nonkombatan; Komcad siber setelah amandemen
Peran TNI	Mengamankan sistem sendiri	Dukungan atas permintaan	OMSP siber oleh Komando Gabungan Siber	Operasi militer siber oleh Komponen Utama
Status hukum peserta sipil	Warga sipil	Warga sipil	Warga sipil; dilarang tindakan ofensif	Warga sipil dilindungi sepanjang tidak berpartisipasi langsung dalam permusuhan

Dimensi	A0 Kompetisi rutin	A1 Krisis siber nasional	A2 Hibrida/zona abu-abu	A3 Konflik bersenjata
Kontrol sipil dan akuntabilitas	Pengawasan regulator; UU PDP	Laporan pascainsiden kepada Presiden dan DPR	Keputusan Presiden; pemberitahuan DPR; klausul kedaluwarsa	Persetujuan DPR; hukum humaniter internasional
Pemicu naik ambang	Dampak lintas sektor IIV yang ditetapkan Kepala BSSN	Atribusi aktor negara oleh <i>fusion center</i> dan keputusan Presiden	Pernyataan darurat militer atau perang dengan persetujuan DPR	–

Sumber: analisis penulis berdasarkan dokumen hukum, Provan dan Kenis (2008), Croissant et al. (2010), dan Schmitt (2017).

Model SSBA bekerja dengan tiga aturan. Pertama, eskalasi kewenangan mengikuti eskalasi ancaman, bukan sebaliknya. Kewenangan militer hanya bertambah bila ambang naik melalui keputusan yang tercatat, sehingga kontrol sipil atas arena keamanan dalam negeri dan pertahanan tetap terjaga (Croissant et al., 2010). Kedua, setiap transisi bersyarat, tercatat waktu, dan dapat diturunkan kembali melalui klausul kedaluwarsa. Pencatatan waktu ini sekaligus menjadi cara mengukur *administrative lag* yang tidak dapat dihitung pada kasus PDNS 2. Ketiga, peran talenta sipil selalu defensif dan nonkombatan pada setiap ambang. Tindakan ofensif hanya dijalankan Komponen Utama, sejalan dengan pelajaran dari *IT Army* Ukraina (Done, 2023; Schmitt, 2017).

Bila diterapkan pada PDNS 2, model ini mengklasifikasikan insiden tersebut sebagai A1, karena gangguannya lintas sektor tetapi tidak ada bukti publik tentang keterlibatan aktor negara. Pada ambang itu, BSSN seharusnya memimpin dengan kewenangan yang mengikat instansi pengguna, termasuk kewajiban pencadangan data, dan talenta sipil dapat dilibatkan melalui pengabdian sesuai profesi, bukan melalui Komponen Cadangan. Klasifikasi ini juga menjelaskan mengapa usulan mobilisasi cadangan siber untuk kasus semacam PDNS 2 keliru sasaran: insiden itu berada dua jenjang di bawah ambang yang dipersyaratkan UU No. 23/2019.

Model SSBA berbeda dari usulan terdahulu dalam tiga hal. Dibandingkan Novrianto et al. (2026), model ini tidak menempatkan DKN sebagai pusat komando untuk semua keadaan, tetapi membatasi peran forum krisis lintas lembaga pada ambang A2. Dibandingkan Pamungkas et al. (2026), model ini tidak memberikan

perlindungan hukum bagi serangan balik oleh warga sipil, tetapi membatasi peran sipil pada fungsi defensif. Dibandingkan Suwandi et al. (2026), model ini menautkan peta jalan angkatan siber dengan gerbang kontrol sipil yang dapat diukur. Model ini juga menanggapi kritik Arif et al. (2024) tentang kekakuan pembagian peran sipil-militer di zona abu-abu: pembagian peran tetap tegas pada setiap ambang, tetapi perpindahan antarambang diatur secara eksplisit.

Sebagai kerangka hipotetis, Model SSBA menurunkan tiga proposisi yang dapat diuji pada penelitian lanjutan. P1: semakin jelas ambang eskalasi yang diatur undang-undang, semakin pendek *administrative lag* pada insiden ambang A1 dan A2. P2: pada jejaring dengan jumlah partisipan besar dan kepercayaan rendah, organisasi pemimpin yang berdasar undang-undang menghasilkan tingkat respons notifikasi (indikator O1) yang lebih tinggi daripada organisasi pemimpin yang berdasar Perpres. P3: pelibatan talenta sipil melalui jalur defensif dan nonkombatan menghasilkan legitimasi publik dan minat partisipasi yang lebih tinggi daripada jalur cadangan militer. Ketiga proposisi ini dapat diuji melalui studi kasus komparatif insiden siber, survei talenta digital, dan simulasi latihan krisis.

Model ini memiliki batas. Penentuan ambang A2 bergantung pada atribusi, padahal atribusi serangan siber sering lambat dan tidak pasti. Pemicu berbasis keputusan Presiden juga berisiko dipolitisasi. Karena itu, model ini mensyaratkan pemberitahuan kepada DPR, klausul kedaluwarsa, dan evaluasi independen (indikator K1) sebagai pengaman. Selain itu, ambang dan pemicu dalam Tabel 9 merupakan usulan konseptual yang perlu diterjemahkan ke dalam rumusan pasal oleh pembentuk undang-undang.

5. Kesimpulan

Penelitian ini bertujuan merekonstruksi Sishankamrata untuk domain siber dengan menguji kelayakan hukum, bukti kasus, pelajaran komparatif, dan peta jalannya. Jawaban atas RQ1: *doctrinal lag* terletak pada ketidaksesuaian antara logika mobilisasi Sishankamrata yang biner dan persaingan siber yang berkelanjutan di

bawah ambang perang, yang tampak pada ketiadaan jalur operasional pelibatan talenta digital sipil. Jalur Komponen Pendukung dan pengabdian sesuai profesi lebih layak daripada Komponen Cadangan, yang terhalang ketiadaan matra siber, batas usia, pelatihan dasar kemiliteran, dan syarat mobilisasi pada darurat militer atau perang. Perbandingan dengan model Nordik, Singapura, Estonia, dan Ukraina menunjukkan bahwa pelibatan sipil yang berhasil membutuhkan dasar hukum khusus dan batas peran defensif.

Jawaban atas RQ2: *governance mismatch* tampak pada BSSN yang tanpa daya paksa, ketiadaan protokol eskalasi, perbedaan klasifikasi informasi, dan koordinasi berjenjang. Secara teoretis, persoalan ini bersumber dari pemakaian mode organisasi pemimpin tanpa kewenangan setingkat undang-undang. Kasus PDNS 2 mengindikasikan kerentanan tata kelola, tetapi *administrative lag*-nya tidak dapat dihitung dari data publik, dan sebagian angka kronologi hanya didukung studi sekunder yang belum diverifikasi. Jawaban atas RQ3: *structural void* dapat diisi melalui Model SSBA, yang memetakan empat ambang ancaman terhadap kewenangan, jalur sipil, mode tata kelola, dan kontrol sipil, serta melalui peta jalan empat tahap dengan jeda evaluasi yang dikendalikan 13 indikator terukur. Pembiayaan menjadi prasyarat, tetapi harus tunduk pada batas hukum, termasuk kewajiban pendanaan TNI dari anggaran negara.

Implikasi kebijakannya ada empat. Pertama, mulai dari jalur yang sudah dimungkinkan hukum, yaitu Komponen Pendukung dan pengabdian sesuai profesi, dengan batas peran defensif. Kedua, prioritaskan undang-undang keamanan dan ketahanan siber yang memuat ambang eskalasi berjenjang, klausul kedaluwarsa, dan partisipasi publik. Ketiga, bangun pengukuran *administrative lag* dengan mencatat waktu deteksi, transisi ambang, dan keputusan lintas lembaga pada setiap insiden. Keempat, validasi ambang indikator gerbang dan pemicu transisi bersama pakar. Keterbatasan penelitian ini adalah penelusuran sumber yang purposif, bukti kasus yang tunggal, perbandingan yang bertumpu pada sumber sekunder, dan model yang

bersifat konseptual. Penelitian lanjutan dapat menguji proposisi P1–P3 melalui studi kasus insiden lain, wawancara pemangku kepentingan, survei talenta digital, dan simulasi biaya.

Daftar Pustaka

1. Buku dan Laporan

- Buffaloe, D. L. (2006). *Defining asymmetric warfare* (Land Warfare Paper No. 58). Institute of Land Warfare, Association of the United States Army.
<https://www.ausa.org/sites/default/files/LWP-58-Defining-Asymmetric-Warfare.pdf>
- George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.
- Huntington, S. P. (1957). *The soldier and the state: The theory and politics of civil-military relations*. Belknap Press of Harvard University Press.
- Kaska, K., Osula, A.-M., & Stinissen, J. (2013). *The Cyber Defence Unit of the Estonian Defence League: Legal, policy and organisational analysis*. NATO Cooperative Cyber Defence Centre of Excellence.
<https://www.ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/>
- Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.
<https://doi.org/10.1017/9781316822524>
- Sørensen, E., & Torfing, J. (Eds.). (2007). *Theories of democratic network governance*. Palgrave Macmillan. <https://doi.org/10.1057/9780230625006>

2. Jurnal

- Achmadi, B., Sarjito, A., & Soebakgijo, N. H. (2025). The future of defense industrialization 5.0 in Indonesia: The potential role of the enforced autonomy model. *Multidisciplinary Science Journal*, 8, Article e2026344.
<https://doi.org/10.31893/multiscience.2026344>
- Adma, A., Surbakti, Y. M., & Sari, P. (2023). Transformasi sistem pertahanan siber Indonesia dengan BSSN sebagai poros & motor penggerak menuju angkatan siber mandiri di masa depan. *Jurnal Kajian Stratejik Ketahanan Nasional*, 6(1), Article 7. <https://doi.org/10.7454/jkskn.v6i1.10077>
- Al Asyari, H. (2023). Between freedom and protection: A critical review of Indonesia's cyberspace law. *Prophetic Law Review*, 5(1), 79–103.
<https://doi.org/10.20885/PLR.vol5.iss1.art5>

- Alzaki, A., Sudirman, A., Sumadinata, R. W. S., Darmawan, W. B., & Aljaafreh, O. M. (2026). National security complex and networked securitization in cognitive warfare. *Nusantara: Journal of Law Studies*, 5(1), 582–601. <https://doi.org/10.66325/nusantaralaw.v5i1.296>
- Arif, M., Afriansyah, A., Chairil, T., & Lestari, G. A. (2024). Grey zone conflict in the South China Sea: The challenges for Indonesian maritime security governance. *Contemporary Southeast Asia*, 46(3), 407–434. <https://doi.org/10.1355/cs46-3c>
- Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International Security*, 26(1), 93–128. <https://doi.org/10.1162/016228801753212868>
- Bachtiar, M., Irwanto, B., Ahmad, I., Sahabuddin, Z. A., & Trismadi. (2026). Defense spending under pressure: An ARDL study of Indonesia's economic and strategic realities. *Statistics, Politics and Policy*, 17(1), 19–42. <https://doi.org/10.1515/spp-2025-0013>
- Baethge, C., Goldbeck-Wood, S., & Mertens, S. (2019). SANRA — A scale for the quality assessment of narrative review articles. *Research Integrity and Peer Review*, 4, Article 5. <https://doi.org/10.1186/s41073-019-0064-8>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Brill, A., & Fairtlough, J. (2020). Fighting the first battle of cyberspace preparedness: Finding your reserve cyber-warriors. *Information & Security: An International Journal*, 44, 9–15. <https://doi.org/10.11610/isij.4401>
- Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43–62. <https://doi.org/10.1111/1468-2346.12504>
- Croissant, A., Kuehn, D., Chambers, P., & Wolf, S. O. (2010). Beyond the fallacy of coup-ism: Conceptualizing civilian control of the military in emerging democracies. *Democratization*, 17(5), 950–975. <https://doi.org/10.1080/13510347.2010.501180>
- Done, W. D. (2023). The Information Technology Army of Ukraine and cyber warfare doctrine. *Journal of Strategic Security*, 16(4), 15–33. <https://doi.org/10.5038/1944-0472.16.4.2127>
- Dunn Cavelty, M., Kaufmann, M., & Soby Kristensen, K. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*, 46(1), 3–14. <https://doi.org/10.1177/0967010614559637>
- Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5–32. <https://doi.org/10.1080/13523260.2019.1678855>

- Floyd, R. (2011). Can securitization theory be used in normative analysis? Towards a just securitization theory. *Security Dialogue*, 42(4–5), 427–439.
<https://doi.org/10.1177/0967010611418712>
- Ginting, R. G., Arifyanto, G. T., & Ghafur, F. (2025). Defending the state in the digital domain: Between cyber threats and national awareness. *Cakrawala: Journal of Citizenship Teaching and Learning*, 3(1), 11–20. <https://doi.org/10.70489/8ybgrr82>
- Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91–108. <https://doi.org/10.1111/j.1471-1842.2009.00848.x>
- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175.
<https://doi.org/10.1111/j.1468-2478.2009.00572.x>
- Harknett, R. J., & Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45(4), 534–567.
<https://doi.org/10.1080/01402390.2020.1732354>
- Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 5(1), Article tyz008.
<https://doi.org/10.1093/cybsec/tyz008>
- Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7–40. https://doi.org/10.1162/ISEC_a_00138
- Kostyuk, N., & Zhukov, Y. M. (2019). Invisible digital front: Can cyber attacks shape battlefield events? *Journal of Conflict Resolution*, 63(2), 317–347.
<https://doi.org/10.1177/0022002717737138>
- Krahmann, E. (2003). Conceptualizing security governance. *Cooperation and Conflict*, 38(1), 5–26. <https://doi.org/10.1177/0010836703038001001>
- Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. *International Affairs*, 92(1), 175–195. <https://doi.org/10.1111/1468-2346.12509>
- Marsudiyanto, A. (2025). Addressing fiscal gap between budget availability and financing needs for Indonesian defense strategies. *Asian Journal of Accounting Research*, 10(4), 430–455. <https://doi.org/10.1108/AJAR-10-2024-0417>
- Marsudiyanto, A., Subroto, A., Brodjonegoro, B. P. S., & Ghafur, A. H. S. (2025). Historical trajectories of Indonesia's fiscal gap and military spending, 2003–2023. *Paramita: Historical Studies Journal*, 35(2), 180–196.
<https://doi.org/10.15294/paramita.v35i2.32010>
- Maschmeyer, L. (2021). The subversive trilemma: Why cyber operations fall short of expectations. *International Security*, 46(2), 51–90.
https://doi.org/10.1162/isec_a_00418

- Matthews, R., Maharani, C., Jupriyanto, & Wu, S. S. (2025). Indonesia's defense acquisition strategy. *Asian Security*, 21(2), 125–148.
<https://doi.org/10.1080/14799855.2025.2527088>
- Novrianto, M., Firman Z, Y. D., & Saptono, E. (2026). The invisible siege: Re-evaluating Indonesia's defense management architecture against transnational non-military threats in the digital era. *Formosa Journal of Multidisciplinary Research*, 5(1), 125–134. <https://doi.org/10.55927/fjmr.v5i1.691>
- Nurtrihadi, A., Jupriyanto, & Waluyo, D. (2025). Development of cyber security system to protect domestic defense industry infrastructure. *International Journal of Integrated Science and Technology*, 3(1), 1241–1252.
<https://doi.org/10.59890/ijist.v3i1.226>
- Pamungkas, R. P., Kustiawan, B., Supriyadi, A. A., & Saputro, G. E. (2026). Fragmentation of authority in national cyber defense: A legal analysis of overlapping inter-agency authority and the urgency of integrated command. *PALAR (Pakuan Law Review)*, 12(1), 105–116.
<https://doi.org/10.33751/palar.v12i1.41>
- Permana, A. (2021). Indonesia's cyber defense strategy in mitigating the risk of cyber warfare threats. *Syntax Idea*, 3(1), 1–11. <https://doi.org/10.46799/syntax-idea.v3i1.860>
- Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, 18(2), 229–252. <https://doi.org/10.1093/jopart/mum015>
- Puspita D., R. A., Persadha, P. D., & Mulyadi. (2025). Analisis ancaman serangan siber pada infrastruktur informasi vital terhadap stabilitas keamanan nasional. *Syntax Literate: Jurnal Ilmiah Indonesia*, 10(5), 5397–5406.
<https://doi.org/10.36418/syntax-literate.v10i5.59084>
- Reksoprodjo, A. H. S. (2026). A C4ISR-integrated framework for critical infrastructure vulnerability assessment in Nusantara Capital City. *Ingénierie des Systèmes d'Information*, 31(7), 2435–2447. <https://doi.org/10.18280/isi.310725>
- Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32.
<https://doi.org/10.1080/01402390.2011.608939>
- Rizki, A., & Timur, F. G. C. (2021). Synergy of multi-stakeholders in defending Indonesia from cyber threats. *Journal of Social Political Sciences*, 2(4), 342–354.
<https://doi.org/10.52166/jsps.v2i4.80>
- Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's cyber security through public-private partnership (PPP). *Central European Journal of International and Security Studies*, 13(4), 104–120. https://www.cejiss.org/images/issue_articles/2019-volume-13-issue-4/07-addressing-indonesia-s-cyber-security-through-public-private-partnership-ppp.pdf

- Saputra, T., Yuharian, R. A., Akbar, M. I., & Augustia, A. E. (2026). Analisis kronologi dan penanganan insiden ransomware pada PDNS 2 sebagai evaluasi strategi keamanan data pemerintah Indonesia. *JRIIN: Jurnal Riset Informatika dan Inovasi*, 3(8), 2305–2309.
<https://jurnalmahasiswa.com/index.php/jriin/article/view/3349>
- Suhirwan, S. (2026). Governing cross-border cyber threat intelligence sharing for maritime security resilience in the Strait of Malacca. *Journal of Contemporary Governance and Public Policy*, 7(1), 107–134.
<https://doi.org/10.46507/jcgpp.v7i1.797>
- Suwandi, Suhardi, Prasetyono, B., Surjatmodjo, D., & Legowo, Y. A. (2026). Strategic intelligence analysis on the urgency of establishing a cyber force in Indonesia. *Journal of Law, Politic and Humanities*, 6(3), 1552–1561.
<https://doi.org/10.38035/jlph.v6i3.3093>
- Syahrial, S. M., Makarim, E., Mahardika, Z. P., & Anggraini, A. G. (2026). Pertanggungjawaban hukum pemerintah terhadap insiden siber kebocoran data pribadi. *Technology and Economics Law Journal*, 5(1), Article 5.
<https://doi.org/10.21143/TELJ.vol5.no1.1075>
- Wibowo, S. E., Hartono, A., Kiswanto, H., Louerens, J. T. A., & Primawanti, H. (2024). Securitization of cyber threats to the Indonesian government: A study of cyber defense strategy. *Global Political Studies Journal*, 8(2), 97–108.
<https://ojs.unikom.ac.id/index.php/gps/article/view/13817>
- Wigell, M. (2019). Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy. *International Affairs*, 95(2), 255–275.
<https://doi.org/10.1093/ia/iiz018>
- Wither, J. K. (2020). Back to the future? Nordic total defence concepts. *Defence Studies*, 20(1), 61–81. <https://doi.org/10.1080/14702436.2020.1718498>
- Wrange, J., Bengtsson, R., & Brommesson, D. (2024). Resilience through total defence: Towards a shared security culture in the Nordic–Baltic region? *European Journal of International Security*, 9, 511–532.
<https://doi.org/10.1017/eis.2024.15>

3. Media Online dan Dokumen Resmi

- Cloudcomputing.id. (2024, 25 Juni). Kronologi serangan ransomware yang lumpuhkan PDN. *Cloudcomputing.id*.
<https://event.cloudcomputing.id/berita/kronologi-serangan-pdn>
- detikINET. (2024, 26 Juni). Ada orang dalam terlibat serangan ransomware di PDNS 2? *detikInet*. <https://inet.detik.com/security/d-7410385/ada-orang-dalam-terlibat-serangan-ransomware-di-pdns-2>
- MCI & MINDEF [Ministry of Communications and Information & Ministry of Defence, Singapore]. (2019, 15 Februari). *Total Defence strengthened with addition*

of Digital Defence as the sixth pillar [Siaran pers bersama].

<https://www.mddi.gov.sg/newsroom/total-defence-strengthened-with-addition-of-digital-defence/>

Nurhakim, F. (2025, 29 Oktober). BSSN catat 3,64 miliar serangan siber selama Januari–Juli 2025. *Bloomberg Technoz*.
<https://www.bloombergtechnoz.com/detail-news/88672/bssn-catat-3-64-miliar-serangan-siber-selama-januari-juli-2025>

4. Peraturan Perundang-undangan

Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara.
<http://peraturan.bpk.go.id/Details/44421/uu-no-3-tahun-2002>

Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.
<http://peraturan.bpk.go.id/Details/40774/uu-no-34-tahun-2004>

Undang-Undang Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara. <https://www.kemhan.go.id/poathan/wp-content/uploads/2020/03/Salinan-UU-Nomor-23-Tahun-2019.pdf>

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

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

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.
<http://peraturan.bpk.go.id/Details/165493/perpres-no-28-tahun-2021>

Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.
<https://peraturan.bpk.go.id/Details/255542/perpres-no-47-tahun-2023>

Tentang Penulis (Penulis Pertama)

Yogi Sugama Takasita Manik memperoleh gelar Sarjana (S1) dan saat ini sedang menempuh pendidikan pascasarjana pada program studi Magister Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan Republik Indonesia. Minat penelitiannya berfokus pada strategi pertahanan, doktrin intelijen, pertahanan siber, serta kontraterorisme dan separatisme. Penulis dapat dihubungi melalui surel: yogidamanik@gmail.com.