JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN
eISSN: 3063-802X ; pISSN: [illegible]
Vol. 3, No. 2, 2026
Hal. 7171-7187
Available online at *https://teewanjournal.com/index.php/juragan*

Kajian Akademis Tata Kelola Dan Manajemen Sumber Daya Buatan: Teknologi Siber Dan Infrastruktur Digital Sebagai Obyek Vital Nasional Dalam Kerangka Undang-Undang Nomor 23 Tahun 2019 Tentang Pengelolaan Sumber Daya Nasional Untuk Pertahanan Negara

Riyanto Wujarso[1*], Surachman Surjaatmadja[2], Imam Tri Wahyudi[3]
Manajemen Pertahanan, Ilmu Pertahanan, Universitas Pertahanan RI, Jakarta, Indonesia[1,2,3]

Email korespondensi[*] riyanto.wujarso@doktoral.idu.ac.id

ARTICLE INFO

Article History:

Submitted 30-07-2026
Received 01-08-2026
Published 05-08-2026

Keywords:

Cyber Governance, Artificial Resources, National Vital Objects, UU PSDN, Systems Thinking;

ABSTRACT

The shift of the state's center of gravity into the digital domain has created new vulnerabilities, where disruptions to cyber infrastructure may lead to national paralysis. This study examines the governance of cyber technology and digital infrastructure as National Vital Objects within the framework of Law No. 23 of 2019 on the Management of National Resources for State Defense (UU PSDN). A systems thinking approach was employed using Causal Loop Diagrams (CLD) and SWOT/TOWS analysis to identify the institutional factors underlying the gap between high cyber threat intensity and weak compliance enforcement. The findings reveal that cyber technology and digital infrastructure conceptually and operationally qualify as Artificial Resources and National Vital Objects but lack legal certainty due to the absence of the Government Regulation mandated by Article 56 of the UU PSDN. This regulatory gap weakens the implementation of Article 59 on asset maintenance and reduces the effectiveness of cyber detection and response mechanisms. The TOWS analysis positions Indonesia in a turn-around strategic posture emphasizing internal institutional consolidation. The study recommends accelerating the issuance of the Government Regulation, harmonizing it with Presidential Regulation No. 82 of 2022, establishing mandatory incident reporting and administrative sanctions, allocating a minimum cybersecurity budget, expediting the Cyber Security and Resilience Bill, and institutionalizing a Cyber Reserve Component through professional partnerships.

ABSTRAK

Pergeseran pusat gravitasi negara ke ranah digital menciptakan kerentanan baru, di mana gangguan terhadap infrastruktur siber berpotensi menimbulkan kelumpuhan nasional. Penelitian ini menganalisis tata kelola teknologi siber dan infrastruktur digital sebagai Objek Vital Nasional dalam kerangka Undang-Undang

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara (UU PSDN). Penelitian menggunakan pendekatan *systems thinking* melalui *Causal Loop Diagram* (CLD) serta analisis SWOT/TOWS untuk mengidentifikasi akar permasalahan kelembagaan yang menyebabkan tingginya ancaman siber namun rendahnya kapasitas penegakan kepatuhan. Hasil penelitian menunjukkan bahwa teknologi siber dan infrastruktur digital secara konseptual maupun faktual memenuhi kriteria sebagai Sumber Daya Buatan dan Objek Vital Nasional, tetapi belum memiliki kepastian hukum karena belum diterbitkannya Peraturan Pemerintah sebagaimana diamanatkan Pasal 56 UU PSDN. Kekosongan regulasi ini melemahkan implementasi Pasal 59 terkait pemeliharaan aset dan menurunkan efektivitas sistem deteksi serta respons. Analisis TOWS menempatkan Indonesia pada strategi *turn-around* yang menekankan konsolidasi internal. Penelitian merekomendasikan percepatan penerbitan Peraturan Pemerintah, harmonisasi regulasi, pelaporan insiden wajib, penguatan anggaran keamanan siber, percepatan RUU Keamanan dan Ketahanan Siber, serta pembentukan Komponen Cadangan Siber berbasis kemitraan profesional.

PENDAHULUAN

Doktrin pertahanan negara Republik Indonesia (RI) menganut Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) yang bertumpu pada asas kesemestaan, kerakyatan, dan kewilayahan sebagaimana diamanatkan Pasal 30 Undang-Undang Dasar Negara RI Tahun 1945 (UUD 1945) dan dijabarkan melalui Undang-Undang (UU) Nomor 3 Tahun 2002 tentang Pertahanan Negara. Di dalam kerangka doktrinal tersebut, UU Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara (UU PSDN) hadir sebagai instrumen operasional yang dimaksudkan untuk mentransformasikan seluruh sumber daya nasional menjadi kekuatan pertahanan melalui pembentukan Komponen Cadangan (Komcad) dan Komponen Pendukung (Komduk). Persoalan mendasar yang dihadapi hari ini adalah bahwa konstruksi Sumber Daya Buatan (SDB) di dalam UU tersebut masih dominan dipahami secara fisik dan material, berupa pabrik, gudang, alat angkut, serta fasilitas produksi, sementara pusat gravitasi penyelenggaraan negara modern telah bergeser secara fundamental ke ranah digital. Ketika sistem pembayaran, administrasi kependudukan, logistik pertahanan, komando dan kendali militer, hingga penyelenggaraan pemilihan umum seluruhnya bertumpu pada sistem elektronik, maka gangguan pada satu simpul jaringan berpotensi menimbulkan kelumpuhan yang setara dengan kehancuran fisik obyek vital konvensional.

Pergeseran tersebut memiliki landasan konseptual yang kuat dalam literatur studi keamanan. Buzan et al. (1998) melalui kerangka sekuritisasi menunjukkan bahwa keamanan bukanlah kondisi obyektif melainkan konstruksi intersubjektif yang terbentuk ketika suatu isu

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

berhasil diangkat sebagai ancaman eksistensial terhadap obyek rujukan tertentu, sehingga membenarkan penggunaan langkah luar biasa di luar prosedur politik normal. Hansen & Nissenbaum (2009) mengembangkan tesis tersebut secara spesifik ke dalam ranah siber dan menunjukkan bahwa keterjalinan antara jaringan teknis, individu pengguna, dan kolektivitas nasional menjadikan ruang siber sebagai sektor keamanan yang memiliki logika tersendiri, di mana gangguan pada lapisan teknis dengan cepat merambat menjadi persoalan kedaulatan dan legitimasi negara. Dengan logika demikian, infrastruktur digital nasional secara konseptual telah memenuhi seluruh kualifikasi untuk ditetapkan sebagai SDB sekaligus Obyek Vital Nasional (Obvitnas) yang wajib dibina, dipelihara, dan dirawat di dalam kerangka pertahanan negara.

Argumen konseptual tersebut memperoleh penegasan empiris dari data pemantauan yang dipublikasikan Badan Siber dan Sandi Negara (BSSN). Sepanjang tahun 2025 BSSN mencatat sekitar 5,2 miliar anomali trafik internet yang berpotensi berkembang menjadi serangan siber, atau setara dengan rata-rata sekitar 182 anomali pada setiap detiknya dengan sekitar 93,78 persen di antaranya berkaitan dengan aktivitas malware yang berpotensi berkembang menjadi ransomware. Yang lebih mengkhawatirkan daripada angka absolutnya adalah laju pertumbuhannya, sebab volume anomali sepanjang satu tahun tersebut disebut telah melampaui akumulasi anomali sepanjang periode 2020 hingga 2024 secara keseluruhan, yang menunjukkan bahwa eskalasi ancaman bersifat eksponensial dan bukan linier. Adapun jenis perangkat lunak berbahaya yang paling banyak terdeteksi meliputi Mirai Botnet, Remcos RAT, dan Generic Trojan dengan pola serangan yang menyasar tidak hanya sistem utama melainkan juga pengguna dan seluruh ekosistem pendukungnya.

Namun temuan yang paling relevan bagi kajian tata kelola justru terletak pada sisi penanganan, bukan pada sisi ancaman. BSSN menyampaikan bahwa sepanjang tahun 2025 BSSN telah menerbitkan 2.855 notifikasi kerawanan, tetapi hanya 2.186 di antaranya memperoleh respons dari pihak terkait; sementara pada paruh pertama tahun 2026 tercatat 776 respons dari 1.002 notifikasi yang dikeluarkan. Pejabat BSSN bahkan secara terbuka menyatakan bahwa Institusi tidak memiliki kewenangan untuk memaksa tindak lanjut apabila notifikasi kerawanan yang telah disampaikan diabaikan oleh Penyelenggara Sistem Elektronik (PSE). Pernyataan tersebut merupakan inti persoalan yang menjadi fokus kajian ini, sebab ia memperlihatkan bahwa persoalan pertahanan siber Indonesia tidak semata-mata bersifat teknis melainkan bersifat institusional dan regulatif. Negara telah memiliki kapabilitas deteksi yang memadai, tetapi tidak memiliki instrumen kepatuhan yang mengikat pada sisi pemeliharaan dan perawatan aset. Kesenjangan antara kapasitas deteksi dan kapasitas penegakan inilah yang secara langsung berkorespondensi dengan kekosongan pengaturan Pasal 56 dan lemahnya operasionalisasi Pasal 59 UU PSDN. Pada saat yang sama, BSSN juga telah mengidentifikasi risiko baru yang bersifat antisipatif berupa perkembangan komputasi kuantum yang diperkirakan mengubah lanskap keamanan siber global, sehingga mulai menyiapkan penerapan *post quantum cryptography sebuah* penegasan bahwa manajemen sumber daya siber tidak dapat

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

dikelola secara reaktif tahunan melainkan harus berbasis peta jalan jangka menengah dan panjang.

Ditinjau dari sisi yuridis, Pasal 51 sampai dengan Pasal 55 UU PSDN mengatur penetapan Sumber Daya Alam (SDA), SDB, serta Sarana dan Prasarana Nasional sebagai Komduk yang dapat ditingkatkan kesiapan untuk kepentingan pertahanan negara, sedangkan Pasal 56 menyatakan bahwa ketentuan lebih lanjut mengenai penetapan tersebut diatur dengan Peraturan Pemerintah (PP). Keterlambatan penerbitan PP dimaksud menimbulkan sekurang-kurangnya tiga implikasi strategis yang saling berkaitan.

Implikasi pertama berupa ketidakpastian status hukum, sebab tanpa penetapan formal maka Pusat Data Nasional (PDN), jaringan tulang punggung serat optik, sistem satelit komunikasi, stasiun pendaratan kabel laut, sistem kendali industri pada obyek vital, serta platform layanan publik digital tidak memiliki kedudukan hukum sebagai SDB yang tunduk pada rezim pembinaan pertahanan negara. Implikasi kedua berupa ketidakjelasan subyek kewajiban, karena Pasal 59 ayat (2) menempatkan tanggung jawab pemeliharaan dan perawatan pada pemilik atau pengelola SDB di bawah supervisi kementerian atau lembaga (K/L) terkait, sehingga apabila obyek belum ditetapkan maka subyek yang dibebani kewajiban pun belum teridentifikasi secara definitif dan supervisi kehilangan pijakan. Implikasi ketiga berupa kekosongan mekanisme pembiayaan dan sanksi, sebab kewajiban pemeliharaan dan perawatan tanpa norma pembiayaan dan tanpa konsekuensi hukum atas kelalaian pada akhirnya hanya akan berhenti sebagai imbauan administratif, persis sebagaimana tercermin dari rendahnya tingkat tindak lanjut notifikasi kerawanan yang telah diuraikan sebelumnya.

Perlu dicatat secara jujur bahwa Indonesia sesungguhnya tidak berada dalam kekosongan regulasi yang absolut. Peraturan Presiden (Perpres) Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital telah menetapkan delapan sektor strategis, yaitu administrasi pemerintahan, energi dan sumber daya mineral, transportasi, keuangan, kesehatan, teknologi informasi dan komunikasi, pangan, serta pertahanan. Perpres tersebut juga telah dilengkapi seperangkat peraturan turunan yang cukup operasional, meliputi Peraturan BSSN Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital, Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital, Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi, Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber, Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber, serta Nomor 5 Tahun 2025 tentang Peta Jalan Pelindungan Infrastruktur Informasi Vital Sektor Administrasi Pemerintahan Tahun 2025 sampai dengan 2029. Persoalannya terletak pada fakta bahwa rezim Perpres tersebut berdiri di atas kerangka keamanan siber, sedangkan rezim UU Nomor 23 Tahun 2019 berdiri di atas kerangka pertahanan negara, dan keduanya hingga kini belum terjalin secara normatif. Akibatnya, Infrastruktur Informasi Vital (IIV) yang telah teridentifikasi belum otomatis berstatus sebagai SDB dalam kerangka pengelolaan sumber daya nasional, dan sebaliknya mekanisme pembinaan Komduk

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

belum memanfaatkan hasil identifikasi yang sesungguhnya telah tersedia. Harmonisasi kedua rezim inilah yang menjadi benang merah sekaligus rekomendasi utama kajian ini.

Bertolak dari uraian tersebut, kajian ini bertujuan untuk mengetahui menjawab tiga isu pokok yang saling berkaitan, yakni bagaimana kondisi faktual tata kelola dan manajemen teknologi siber serta infrastruktur digital sebagai Obvitnas apabila ditinjau dari amanat Pasal 51 sampai dengan Pasal 56 dan Pasal 59 UU PSDN; bagaimana konfigurasi kekuatan, kelemahan, peluang, dan ancaman dalam penyelenggaraan tata kelola tersebut; serta strategi dan opsi kebijakan apa yang dapat direkomendasikan kepada pengambil keputusan, khususnya sebagai bahan pelaksanaan fungsi pengawasan Komisi I Dewan Perwakilan Rakyat Republik Indonesia (DPR RI) terhadap mitra kerja Kementerian Pertahanan (KEMHAN), Kementerian Komunikasi dan Digital (KOMDIGI), serta BSSN.

METODE PENELITIAN

Kompleksitas persoalan tata kelola siber nasional bersifat dinamis dan ditandai oleh umpan balik, keterlambatan waktu, serta resistensi kebijakan, maka kajian ini menggunakan pendekatan *system thinking* sebagai kerangka analisis. Sterman (2000) menjelaskan bahwa kebijakan yang dirancang tanpa memahami struktur umpan balik suatu sistem cenderung menghasilkan *policy resistance* yaitu kondisi ketika intervensi justru diserap oleh sistem dan pada akhirnya memperburuk keadaan yang hendak diperbaiki. Senge (1990) dan Meadows (2008) menegaskan bahwa titik ungkit yang paling kuat umumnya terletak pada perubahan aturan main, struktur informasi, dan paradigma sistem, dan bukan pada penambahan parameter seperti anggaran semata.

Berdasarkan kerangka tersebut, variabel-variabel kunci beserta indikator dan rujukan teoritis diuraikan pada tabel berikut, untuk selanjutnya dipetakan hubungan sebab-akibatnya dalam bentuk *Causal Loop Diagram* (CLD).

Tabel 1. Variabel, Indikator, dan Rujukan Teoritis

Variabel	Indikator/Ukuran	Rujukan Teoritis
Investasi Teknologi dan Anggaran Siber (X_1)	Rasio belanja keamanan siber terhadap total belanja Teknologi Informasi Komunikasi (TIK) K/L; nilai pengadaan perangkat deteksi dan respons; cakupan modernisasi *legacy systems*.	Barney (1991); Sterman (2000)
Kesiapan dan Kapasitas SDM Siber (X_2)	Rasio analis siber per 10.000 penduduk/ per instansi; jumlah personel bersertifikasi;	Peraturan BSSN No.

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Variabel	Indikator/Ukuran	Rujukan Teoritis
	tingkat *turnover*; jumlah lulusan bidang keamanan siber	9/2023; ITU (2021)
Kematangan Tata Kelola (X_3)	Skor Indeks Keamanan Informasi (KAMI); tingkat kematangan berdasarkan NIST CSF 2.0; jumlah *Computer Security Incident Response Team* (CSIRT) sektoral aktif; kepatuhan *International Organization for Standardization/ International Electrotechnical Commission* (ISO/IEC) 27001	NIST (2024); Peraturan BSSN No. 10/2023
Kerentanan Sistem (Y_1)	Jumlah notifikasi kerawanan yang belum ditindaklanjuti; jumlah celah kritis belum ditambal; usia rata-rata *legacy systems*; ketergantungan vendor tunggal	BSSN (2026); Woods. (2006)
Intensitas Ancaman (Y_2)	Jumlah anomali trafik per tahun; proporsi malware/ransomware; jumlah dugaan insiden pada sektor IIV	BSSN (2024)
Dampak Insiden (Y_3)	Durasi gangguan layanan publik (*downtime*); volume data terekspos; estimasi kerugian ekonomi; derajat penurunan kepercayaan publik	Dunn Cavelty (2013)
Ketahanan Siber Nasional (Z)	*Mean Time to Detect* (MTTD) dan *Mean Time to Respond* (MTTR); tingkat pemulihan layanan; skor GCI; kesinambungan layanan esensial	ITU (2021); Weick & Sutcliffe (2007)

Struktur Analisisis Umpan Balik

CLD disusun untuk memetakan hubungan sebab-akibat antar variabel dengan menggunakan notasi polaritas positif untuk perubahan searah, dan polaritas negatif untuk

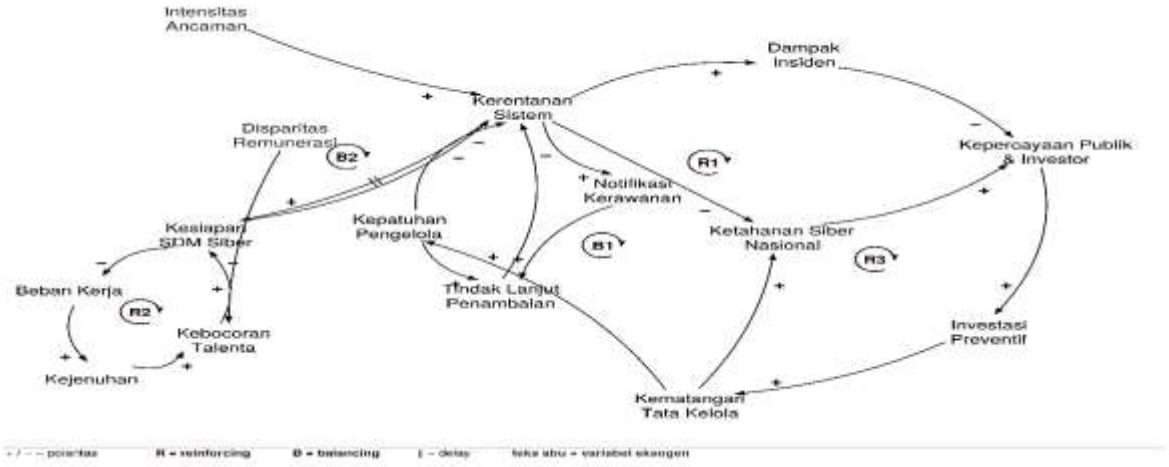
eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

perubahan berlawanan. Struktur umpan balik yang teridentifikasi divisualisasikan pada Gambar 1 meliputi:

1. Lingkaran Penguat Kerentanan (R_1 - Siklus Terluar)
   Meningkatnya Intensitas Ancaman (Y_2) mendorong bertambahnya jumlah eksploitasi terhadap celah keamanan sehingga Kerentanan Sistem (Y_1) yang tereksploitasi ikut meningkat dengan polaritas searah; naiknya kerentanan menaikkan Dampak Insiden (Y_3) dengan polaritas searah pula; membesar dampak insiden menurunkan kepercayaan publik dan investor terhadap layanan digital dengan polaritas berlawanan; menurunnya kepercayaan tersebut, disertai tekanan politik jangka pendek untuk memulihkan layanan secepatnya, mendorong realokasi anggaran ke penanganan reaktif sehingga Investasi Preventif (X_1) justru menurun; menurunnya investasi preventif membuat Kematangan Tata Kelola (X_3) stagnan; stagnasi tata kelola menurunkan tingkat Kepatuhan Pengelola dalam menindaklanjuti kerawanan; dan rendahnya kepatuhan pada gilirannya kembali menaikkan Kerentanan Sistem (Y_1) dengan polaritas berlawanan. Karena jumlah polaritas berlawanan di dalam lingkaran genap, maka lingkaran tersebut bersifat menguat (R_1). Sifat menguat inilah yang menjelaskan mengapa pola penanganan yang bersifat pemadam kebakaran tidak pernah berhasil menurunkan kerentanan struktural: setiap insiden justru menyedot sumber daya yang seharusnya dialokasikan untuk mencegah insiden berikutnya.
2. Lingkaran Penyeimbang Deteksi dan Respons (B_1 - Siklus Tengah)
   Meningkatnya Kerentanan Sistem (Y_1) memicu bertambahnya notifikasi kerawanan yang diterbitkan otoritas siber sehingga tindak lanjut penambalan oleh pengelola meningkat, dan meningkatnya tindak lanjut tersebut pada akhirnya menurunkan kembali Kerentanan Sistem (Y_1). Efektivitas lingkaran sepenuhnya ditentukan oleh satu variabel moderasi yaitu tingkat kepatuhan pengelola. Karena sebagian signifikan notifikasi tidak memperoleh respons dan otoritas siber tidak memiliki kewenangan memaksa, maka penguatan lingkaran B_1 melemah secara struktural.
3. Lingkaran SDM dan Keterlambatan Waktu (R_2 - Siklus Kiri)
   Struktur pertama bersifat menyeimbangkan namun disertai keterlambatan waktu (*time delay*) yang signifikan (3–5 tahun) antara keputusan investasi pendidikan dengan tersedianya analis siber kompeten. Keterlambatan struktural tersebut menyebabkan pengambil kebijakan cenderung kurang berinvestasi pada SDM. Struktur kedua bersifat menguat (R_2): melebarnya disparitas remunerasi antara sektor publik dan swasta meningkatkan perpindahan talenta siber keluar dari instansi pemerintah, menurunkan Kesiapan SDM Siber (X_2) publik, meningkatkan beban kerja personel tersisa, menimbulkan kejenuhan (*burnout*), dan mendorong perpindahan talenta berikutnya.

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Gambar 1. CLD Tata Kelola dan Manajemen SDB Bidang Teknologi Siber dan Infrastruktur



Digital

Sumber: Diolah penulis (2026) berdasarkan Sterman (2000), Meadows (2008), dan data BSSN

HASIL DAN PEMBAHASAN

Lingkungan Strategis

Pada tataran global, lingkungan strategis ditandai oleh kompetisi teknologi antara Amerika Serikat (AS) dan Republik Rakyat Tiongkok (RRT) yang berimplikasi langsung pada fragmentasi rantai pasok semikonduktor, perangkat jaringan, dan layanan komputasi awan. Kondisi tersebut menempatkan negara-negara dengan ketergantungan teknologi tinggi, termasuk Indonesia, pada posisi yang rentan terhadap apa yang di konseptualkan sebagai jalinan yang dipersenjatai, yakni pemanfaatan posisi sentral suatu aktor dalam jejaring global sebagai instrumen tekanan geopolitik. Pada saat yang bersamaan, norma internasional di ruang siber belum mengikat secara hukum: Kelompok Ahli Pemerintah Perserikatan Bangsa-Bangsa (PBB) dan *Open-Ended Working Group* memang telah menyepakati sejumlah norma perilaku negara yang bertanggung jawab, namun kepatuhan bersifat sukarela dan mekanisme atribusi kolektif belum tersedia. Dalam kondisi normatif yang belum matang tersebut, (Nye, 2011, 2017) menilai bahwa penangkalan melalui penyangkalan menjadi pilihan yang paling rasional bagi negara berkekuatan menengah seperti Indonesia. Dimensi teknologi disruptif menambah kompleksitas lingkungan global: perkembangan kecerdasan artifisial generatif telah menurunkan hambatan masuk bagi pelaksanaan serangan siber sekaligus memperluas skala operasi pengaruh berbasis disinformasi, sementara kemajuan komputasi kuantum menghadirkan risiko pemanenan data terenkripsi pada hari ini untuk didekripsi di kemudian hari. Kesadaran otoritas siber nasional untuk mulai menyiapkan kriptografi pasca-kuantum karenanya merupakan langkah antisipatif yang perlu memperoleh dukungan penganggaran multitahun, bukan penganggaran tahunan yang mudah tergerus.

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Pada tataran regional, dinamika Laut China Selatan (LCS) telah meluas dari domain maritim ke domain siber melalui aktivitas *Advanced Persistent Threat* yang menyasar kementerian luar negeri (Kemlu), lembaga pertahanan, dan sektor energi negara-negara pengklaim. Perhimpunan Bangsa-Bangsa Asia Tenggara (ASEAN) sesungguhnya telah membangun sejumlah instrumen kerja sama yang cukup memadai, antara lain *ASEAN Cybersecurity Cooperation Strategy, ASEAN Ministerial Conference on Cybersecurity, ASEAN-Singapore Cybersecurity Centre of Excellence*, serta *ASEAN-Japan Cybersecurity Capacity Building Centre*. Namun kerja sama tersebut menghadapi kendala klasik berupa prinsip non-intervensi, pengambilan keputusan berbasis konsensus, dan disparitas kapasitas antarnegara anggota yang cukup lebar, sehingga kesepakatan cenderung berhenti pada tataran deklaratif. Indonesia, sebagai negara dengan populasi digital terbesar di kawasan, sesungguhnya memiliki modal legitimasi yang cukup untuk memainkan peran kepemimpinan normatif di forum-forum tersebut, sepanjang kapasitas domestik sendiri kredibel dan dapat dipertanggungjawabkan.

Pada tataran nasional, akselerasi transformasi digital pemerintahan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) dan konsolidasi PDN telah menciptakan efisiensi yang nyata, namun sekaligus menghasilkan konsentrasi risiko. Konsolidasi infrastruktur pada hakikatnya melahirkan titik kegagalan tunggal yang apabila terganggu, berdampak lintas sektor secara simultan; dan insiden gangguan pada infrastruktur digital publik serta layanan esensial yang terjadi dalam beberapa tahun terakhir telah menegaskan bahwa ketahanan siber bukan lagi sekadar fitur pendukung melainkan fondasi bagi keberlanjutan ekonomi digital dan pelayanan publik. Secara kelembagaan, terdapat sedikitnya lima aktor dengan kewenangan yang saling bersinggungan, yaitu BSSN sebagai koordinator keamanan siber nasional, Kemhan bersama Pusat Siber Tentara Nasional Indonesia (TNI) pada domain pertahanan, Komdigi pada domain infrastruktur dan tata kelola informasi, Kepolisian Negara Republik Indonesia (Polri) pada penegakan hukum siber, serta regulator sektoral seperti Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) pada sektor keuangan.

Fragmentasi tersebut menimbulkan biaya koordinasi yang tinggi dan zona abu-abu kewenangan, terutama pada fase eskalasi ketika suatu insiden bergeser dari kategori tindak pidana menjadi kategori ancaman pertahanan. Belum tuntasnya pembahasan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS) menyebabkan penataan kewenangan tersebut masih bertumpu pada instrumen setingkat Perpres yang secara hierarkis tidak cukup kuat untuk membebankan kewajiban dan menjatuhkan sanksi kepada badan usaha swasta pengelola Obvitas. Dari perspektif Komisi I DPR RI, konfigurasi tersebut justru menempatkan fungsi pengawasan pada posisi yang sangat strategis, sebab Komisi I DPR RI bermitra dengan Kemhan, Komdigi, serta BSSN, sehingga memiliki kapasitas kelembagaan untuk mendorong harmonisasi lintas mitra kerja melalui instrumen rapat kerja (Raker), pembahasan Rencana Kerja dan Anggaran (RKA), maupun inisiatif legislasi.

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Analisis *Strengths, Weaknesses, Opportunities, Threat (SWOT)*

Bertolak dari pemetaan lingkungan strategis tersebut, analisis SWOT disusun mengikuti kerangka David & David (2017) serta Rangkuti (2015) dengan faktor internal merujuk pada kapasitas kelembagaan negara dan faktor eksternal merujuk pada dinamika global, regional, serta nasional sebagaimana telah diuraikan. Hasil identifikasi keempat faktor tersebut disajikan dalam bentuk matriks berikut.

Tabel 2. Matriks SWOT Tata Kelola dan Manajemen Infrastruktur Digital sebagai Obvitnas

Kekuatan *(Strengths)*	Kelemahan (*Weaknesses*)
S1. Tersedianya payung hukum yang relatif lengkap: UU No. 23/2019 (PSDN), UU No. 27/2022 (PDP), UU No. 11/2008 jo. UU No. 19/2016 jo. UU No. 1/2024 (ITE), serta Perpres No. 82/2022 tentang Pelindungan Infrastruktur Informasi Vital.	W1. Belum terbitnya Peraturan Pemerintah sebagai amanat Pasal 56 UU PSDN untuk penetapan SDB, sehingga aset siber belum memiliki status hukum sebagai komponen pendukung/cadangan.
S2. Eksistensi kelembagaan yang mapan: BSSN sebagai koordinator keamanan siber nasional (Perpres No. 28/2021), Pusat Siber TNI, serta Direktorat Jenderal Pothan Kemhan.	W2. Fragmentasi kewenangan dan tumpang tindih tusi antara BSSN, Komdigi, Kemhan/TNI, Polri, dan regulator sektoral; tidak ada satu pun otoritas dengan kewenangan pemaksa (*enforcement power*).
S3. Kapabilitas deteksi dini nasional melalui monitoring trafik 24/7 dan ekosistem CSIRT sektoral serta *Gov-CSIRT*.	W3. Rendahnya tingkat kepatuhan penyelenggara IIV terhadap notifikasi kerawanan; sebagian besar notifikasi tidak ditindaklanjuti secara tuntas.
S4. Kerangka teknis turunan yang operasional: Peraturan BSSN No. 7/2023 (Identifikasi IIV), No. 8/2023 (Kerangka Kerja PIIV), No. 9/2023 (SDM), No. 10/2023 (Indeks KAMI/kematangan), dan No. 1/2024 (Pengelolaan Insiden Siber).	W4. Defisit SDM siber baik kuantitas maupun kualitas, disertai tingginya perpindahan talenta dari sektor publik ke sektor swasta akibat disparitas remunerasi.
S5. Basis demografi digital yang besar dan tumbuhnya talenta siber muda,	W5. Ketergantungan tinggi pada perangkat keras, perangkat lunak, dan layanan awan asing (*supply chain dependency*), serta

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

serta dukungan politik lintas fraksi di Komisi I DPR RI terhadap agenda kedaulatan digital.	minimnya kemandirian kriptografi Nasional. W6. Belum optimalnya alokasi anggaran keamanan siber sebagai persentase belanja TIK K/L, dan lemahnya perencanaan pemeliharaan/perawatan (Pasal 59 UU PSDN) yang bersifat siklikal.
Peluang *(Opportunities)*	Ancaman *(Threats)*
O1. Momentum penyusunan Peraturan Pemerintah turunan UU PSDN dan wacana penguatan RUU KKS sebagai instrumen konsolidasi kewenangan. O2. Pertumbuhan ekonomi digital nasional yang menjadi insentif ekonomi bagi investasi keamanan siber sektor swasta. O3. Terbukanya kerja sama internasional: *ASEAN Regional Forum, ASEAN Cybersecurity Cooperation Strategy, ASEAN-Japan Cybersecurity Capacity Building Centre*, dan kemitraan *bilateral capacity building*. O4. Sinergi *triple helix* dengan perguruan tinggi (Universitas Pertahanan RI, Poltek SSN) dan industri untuk riset, sertifikasi, serta pembentukan Komcad Siber. O5. Adopsi kerangka internasional yang telah teruji (NIST CSF 2.0, ISO/IEC 27001, MITRE *Adversarial*	T1. Meningkatnya volume dan kompleksitas anomali trafik serta serangan berbasis malware, ransomware, dan botnet terhadap infrastruktur digital nasional. T2. Aktivitas *Advanced Persistent Threat* (APT) yang disponsori aktor negara dengan motif spionase strategis terhadap sektor pertahanan dan pemerintahan. T3. *Weaponization of interdependence*: pemanfaatan simpul jaringan global (kabel laut, rantai pasok cip, layanan awan) sebagai instrumen tekanan geopolitik. T4. Ancaman disruptif teknologi baru: serangan berbantuan kecerdasan artifisial, deepfake untuk operasi pengaruh, serta risiko kriptanalisis pasca-kuantum (*harvest now, decrypt later*). T5. Kerentanan faktor manusia dan pihak ketiga (vendor) sebagai vektor dominan insiden, termasuk rekayasa sosial dan penipuan digital berskala masif.

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Tactics, Techniques, & Common Knowledge /ATT&CK) sebagai dasar standardisasi nasional yang cepat dan *legitimate*.	

Pembacaan atas matriks tersebut memperlihatkan sebuah pola yang konsisten dengan temuan analisis *sistem thinking* sebelumnya. Kekuatan yang dimiliki Indonesia bersifat regulatif dan kelembagaan, sedangkan kelemahannya bersifat operasional dan struktural, sementara peluang eksternal relatif terbuka lebar, ancaman eksternal justru bereskalasi dengan kecepatan yang melampaui kecepatan konsolidasi internal. Dengan kata lain, Indonesia tidak kekurangan kerangka hukum maupun lembaga, melainkan kekurangan daya ikat dan daya paksa atas kerangka yang telah dimilikinya.

Strategi Berdasarkan Persilangan Matriks TWOS

Persilangan antara faktor internal dan faktor eksternal menghasilkan empat kelompok strategi turunan yang disajikan dalam matriks TOWS berikut, meliputi strategi agresif yang memanfaatkan kekuatan untuk merebut peluang, strategi pemulihan yang memanfaatkan peluang untuk menutup kelemahan, strategi diversifikasi yang memanfaatkan kekuatan untuk menghadapi ancaman, serta strategi defensif yang meminimalkan kelemahan sekaligus menghindari ancaman.

Tabel 3. Matriks TOWS Perumusan Strategi

Faktor internal / Eksternal	Kekuatan (S)	Kelemahan (W)
PELUANG (O)	STRATEGI S-O (*Agresif/Ekspansif*): SO-1. Melembagakan Komcad Siber (Cyber Reserve) dengan memanfaatkan payung UU PSDN (S1) dan talenta digital nasional (S5, O4) melalui skema pengabdian profesional paruh waktu. SO-2. Mengakselerasi penerbitan PP amanat Pasal 56 UU PSDN	STRATEGI W-O (*Turn-around*): WO-1. Menutup kekosongan hukum W1 melalui penyusunan PP PSDN sektor SDB yang mengatur registrasi, pembinaan, pemeliharaan, dan perawatan aset siber (O1). WO-2. Membangun skema beasiswa ikatan dinas dan jenjang karier fungsional

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Faktor internal / Eksternal	Kekuatan (S)	Kelemahan (W)
	yang secara eksplisit menetapkan IIV digital sebagai SDB (S1, O1). SO-3. Menjadikan kerangka BSSN (S4) sebagai standar wajib nasional yang diharmonisasikan dengan NIST CSF 2.0 dan ISO/IEC 27001 (O5). SO-4. Mengoptimalkan CSIRT sektoral (S3) sebagai simpul kerja sama berbagi informasi ancaman regional ASEAN (O3).	Sandiman/analis siber bersama perguruan tinggi untuk mengatasi defisit SDM (W4, O4). WO-3. Mendorong kemitraan pemerintah–swasta (PPP) pembiayaan keamanan siber IIV dengan insentif fiskal untuk mengurangi beban APBN (W6, O2). WO-4. Menyusun peta jalan kemandirian teknologi dan kriptografi nasional secara bertahap melalui alih teknologi dan offset industri pertahanan (W5, O3).
ANCAMAN (T)	STRATEGI S-T (*Diversifikasi/Diferensiasi*): ST-1. Membangun postur pertahanan siber berlapis (*defence in depth*) dan doktrin *active cyber defence* terbatas dengan memanfaatkan kapabilitas Pusat Siber TNI dan BSSN (S2, S3) terhadap ancaman APT (T2). ST-2. Menyelenggarakan *National Cyber Exercise* dan uji ketahanan (*red teaming*) secara periodik pada seluruh sektor IIV sebagai wujud pemeliharaan dan	STRATEGI W-T (*Defensif*): WT-1. Membentuk mekanisme komando dan koordinasi tunggal (*single national cyber command and control*) dengan pembagian peran yang tegas antara BSSN, Kemhan/TNI, Komdigi, dan Polri untuk menghapus fragmentasi (W2, T1). WT-2. Menetapkan kewajiban pelaporan insiden dan sanksi administratif yang mengikat bagi penyelenggara IIV yang

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Faktor internal / Eksternal	Kekuatan (S)	Kelemahan (W)
	perawatan Pasal 59 UU PSDN (S4, T1).	mengabaikan notifikasi kerawanan (W3, T1).
	ST-3. Menyusun peta jalan migrasi *post-quantum cryptography* dan tata kelola AI keamanan siber sebagai antisipasi ancaman disruptif (S2, T4).	WT-3. Menerapkan manajemen risiko rantai pasok TIK, termasuk *vendor screening* dan pembatasan penggunaan teknologi berisiko tinggi pada IIV pertahanan (W5, T3).
	ST-4. Memperkuat literasi dan budaya keamanan siber aparatur serta masyarakat untuk memitigasi vektor manusia (S5, T5).	WT-4. Menetapkan anggaran minimum keamanan siber (*mandatory floor*) sebagai persentase belanja TIK setiap K/L pengelola IIV (W6, T1).

Keempat kelompok strategi tersebut tidak dapat dilaksanakan secara serentak mengingat keterbatasan sumber daya dan kapasitas kelembagaan, sehingga diperlukan penahapan berdasarkan bobot urgensi dan keterhubungannya dengan titik ungkit yang telah diidentifikasi melalui CLD. Prioritas jangka pendek jatuh pada strategi WO-1 berupa percepatan penerbitan PP amanat Pasal 56 dan strategi WT-2 berupa penetapan kewajiban pelaporan insiden beserta sanksi administratif, karena keduanya secara langsung mengaktifkan kembali lingkaran penyeimbang B1 yang saat ini lumpuh dan karenanya memberikan pengaruh terbesar dengan biaya paling rendah. Prioritas jangka menengah diarahkan pada strategi WT-1 berupa konsolidasi komando dan koordinasi, serta strategi WO-2 dan WT-4 berupa reformasi SDM dan penetapan anggaran minimum yang bersama-sama memutus lingkaran penguat R1 dan R2. Prioritas jangka panjang diarahkan pada strategi SO-1 berupa pelembagaan Komcad Siber, strategi WO-4 berupa pembangunan kemandirian teknologi dan kriptografi, serta strategi ST-3 berupa migrasi menuju kriptografi pasca-kuantum yang seluruhnya menuntut kesinambungan anggaran lintas periode pemerintahan.

KESIMPULAN

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Berdasarkan hasil penelitian, teknologi siber dan infrastruktur digital secara konseptual telah memenuhi kualifikasi sebagai Sumber Daya Pertahanan (SDP) dan Objek Vital Nasional (Obvitnas) dalam kerangka UU PSDN. Penetapan formal belum dapat dilakukan karena peraturan pemerintah sebagaimana diamanatkan dalam Pasal 56 belum diterbitkan. Kondisi tersebut menimbulkan kekosongan hukum yang melemahkan pelaksanaan pembinaan, pemeliharaan, pengawasan, serta penegakan kewajiban keamanan siber. Kapasitas Indonesia dalam mendeteksi ancaman telah berkembang, tetapi efektivitas pertahanan siber masih terkendala rendahnya kepatuhan, lemahnya penegakan hukum, fragmentasi kewenangan, keterbatasan sumber daya manusia, dan ketergantungan terhadap rantai pasok teknologi.

Analisis *system thinking* dan SWOT menunjukkan bahwa peningkatan anggaran serta kapasitas teknologi belum cukup untuk memperbaiki sistem tanpa pembenahan regulasi, tata kelola, dan koordinasi kelembagaan. Strategi prioritas perlu diarahkan pada konsolidasi regulasi dan kewenangan, penguatan kapasitas sumber daya manusia, serta peningkatan kepatuhan sebelum memperluas kapabilitas dan kerja sama internasional. Penetapan infrastruktur digital sebagai sumber daya pertahanan juga dapat mendukung pelibatan masyarakat dalam bela negara di ruang siber melalui skema Komcad dan Komduk. Penerapan Sishankamrata di era digital menuntut penguatan kemampuan kognitif dan teknologi masyarakat dengan tetap menjunjung supremasi sipil, akuntabilitas demokratis, serta perlindungan data pribadi.

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2024). Lanskap keamanan siber Indonesia tahun 2023. Badan Siber dan Sandi Negara Republik Indonesia. https://www.bssn.go.id

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Buzan, B., Waever, O., & de Wilde, J. (1998). Security: A New Framework for Analysis. *Security. A New Framework for Analysis*, 1–28. https://books.google.com/books/about/Security.html?id=j4BGr-Elsp8C

David, F. R., & David, F. R. (2017). *Strategic management: A competitive advantage approach, concepts and cases* (16th ed.). Pearson Education.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, *15*(1), 105–122. https://doi.org/10.1111/misr.12023

Forrester, J. W. (1961). Industrial dynamics. MIT Press.

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

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020*. International Telecommunication Union. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html

Meadows, D. H. (2008). *Thinking in systems: A primer* (D. Wright, Ed.). Chelsea Green Publishing.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Nye, J. S. (2011). *The future of power*. PublicAffairs.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44–71. https://doi.org/10.1162/ISEC_A_00266

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press. https://doi.org/10.1017/CBO9780511807763

Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber. https://peraturan.bpk.go.id

Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2025 tentang Peta Jalan Pelindungan Infrastruktur Informasi Vital Sektor Administrasi Pemerintahan Tahun 2025–2029. https://peraturan.bpk.go.id/Details/315044

Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital. https://peraturan.bpk.go.id

Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital. https://peraturan.bpk.go.id

Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi. https://peraturan.bpk.go.id

Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. https://peraturan.bpk.go.id

Rangkuti, F. (2015). *Analisis SWOT: Teknik membedah kasus bisnis*. PT Gramedia Pustaka Utama.

Rhodes, R. A. W. (1997). *Understanding governance: Policy networks, governance, reflexivity and accountability*. Open University Press.

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

Senge, P. M. (1990). *The fifth discipline: The art and practice of the learning organization*. Doubleday/Currency.

Sterman, J. D. (2000). *Business dynamics: Systems thinking and modeling for a complex world*. Irwin/McGraw-Hill.

Undang-Undang Republik Indonesia Nomor 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara. https://peraturan.bpk.go.id/Details/122032

eISSN 3063-802X & pISSN 3063-
JURAGAN
JURNAL RAGAM PENGABDIAN - PENELITIAN

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798

Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara. https://peraturan.bpk.go.id

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, *5*(2), 171–180. https://doi.org/10.1002/smj.4250050207

Woods, D. (2006). *Resilience engineering: Concepts and precepts* (E. Hollnagel, D. D. Woods, & N. Leveson, Eds.). Ashgate Publishing.