Original Article

e-XXXX-XXXX

Original Article

Penguatan Satuan Siber TNI Guna Menghadapi Ancaman Cyber Warfare Dalam Rangka Meningkatkan Strategi Pertahanan Negara

Burhan Fajari Arfian[1]✉
[1,2,3]Universitas Pertahanan RI, Indonesia
Korespondensi Author: burhan970093@gmail.com

Abstrak:

The rapid development of digital technology has transformed cyberspace into a strategic domain of national defense. The Indonesian National Army (TNI) faces increasingly complex cyber threats, including digital espionage, command system breaches, and cyber-propaganda attacks. This study aims to analyze the strengthening of the TNI Cyber Unit in facing cyber warfare through three main focuses: the role of the Cyber Unit, inter-service interoperability, and strategies for strengthening command and control systems. This research employed a qualitative descriptive method through literature study, in-depth interviews, and SWOT analysis. The results indicate that the TNI Cyber Unit plays a strategic role as the frontline of national digital defense through early detection, network protection, and active cyber operations. However, several challenges remain, including cyber human-resource capability gaps, communication system integration, and digital infrastructure modernization. Therefore, strengthening strategies must prioritize personnel capacity development, C4ISR integration, and full digitalization of the command system supported by artificial intelligence. The study concludes that strengthening the TNI Cyber Unit is essential to reinforce Indonesia's defense strategy and ensure information superiority in the era of digital warfare.

Keywords: TNI Cyber Unit, Cyber Warfare, National Defense, Interoperability, Command and Control

Pendahuluan

Perkembangan teknologi informasi telah mendorong perubahan signifikan dalam karakter ancaman terhadap keamanan nasional, di mana domain siber menjadi arena baru bagi kompetisi dan konflik antarnegara. Cyber warfare kini dipandang sebagai bentuk peperangan modern yang memanfaatkan kerentanan digital untuk melumpuhkan sistem komando dan kendali, mengganggu infrastruktur kritis, serta merusak stabilitas suatu negara tanpa perlu melakukan serangan fisik. Dalam konteks pertahanan negara, strategi pertahanan modern menuntut pendekatan yang adaptif, lintas sektor, serta terintegrasi dengan kemampuan teknologi informasi. Doktrin

Received: November 19, 2025 – Revised: November 25, 2025 - Accepted: Desember 21, 2025 - Published online: January 30, 2026

Pertahanan Negara menegaskan bahwa kekuatan pertahanan tidak lagi hanya bersandar pada komponen militer konvensional, tetapi juga harus mampu menjawab dinamika ancaman non-fisik yang bersifat transnasional, cepat, dan sulit diprediksi. Sejalan dengan itu, Kusumaatmadja (1993) menegaskan bahwa pertahanan nasional harus dibangun melalui sinergi multidimensi yang mencakup aspek politik, ekonomi, sosial, budaya, dan teknologi.

Realitas ancaman siber terhadap Indonesia tampak nyata dari berbagai insiden yang menyerang aset digital pemerintah, sektor strategis, dan simbol pertahanan nasional. Laporan Kementerian Komunikasi dan Informatika pada tahun 2011 mencatat bahwa situs pemerintah berakhiran *.go.id* mengalami ratusan ribu hingga jutaan upaya peretasan setiap tahun, mulai dari defacement, probing, hingga eksploitasi kerentanan sistem. Serangan defacement besar pada 2013 oleh kelompok "Anonymous Indonesia" yang menembus puluhan situs pemerintah memperlihatkan lemahnya perlindungan keamanan aplikasi web instansi publik. Periode 2016–2017 menunjukkan eskalasi serangan yang lebih terkoordinasi, termasuk meningkatnya aktivitas malware dan DDoS terhadap sektor keuangan nasional serta peretasan situs resmi Telkomsel pada 2017. Insiden tersebut berdampak langsung terhadap kepercayaan publik, stabilitas sistem digital nasional, dan kesiapan institusi dalam menjaga keamanan informasinya.

Gangguan terhadap simbol pertahanan nasional juga terjadi pada tahun 2022 ketika situs resmi TNI AD dan Kostrad diretas kelompok "Indian Cyber Mafia" yang memunculkan pesan provokatif pada laman utama. Meskipun tidak ada kebocoran data strategis, insiden ini menunjukkan bahwa domain siber telah menjadi arena yang memengaruhi persepsi publik dan citra institusi pertahanan. Rangkaian insiden tersebut menegaskan adanya ketimpangan antara das sein, yaitu kondisi aktual ketahanan siber nasional yang masih rentan, dengan das sollen yang menuntut sistem pertahanan negara adaptif terhadap pola ancaman baru yang bersifat non-teritorial, masif, dan simultan. Kondisi ini menggambarkan urgensi untuk memperkuat postur pertahanan digital melalui strategi yang lebih terstruktur, lintas lembaga, serta berorientasi jangka panjang.

Pemerintah telah merespons dinamika tersebut melalui pembentukan Badan Siber dan Sandi Negara (BSSN) melalui Peraturan Presiden Nomor 53 Tahun 2017 untuk memperkuat perlindungan infrastruktur informasi vital nasional. Di lingkungan militer, TNI membentuk Satuan Siber TNI sebagai upaya meningkatkan kemampuan pertahanan di domain siber melalui pengembangan organisasi, peningkatan kualitas sumber daya manusia, serta penguatan sistem komando dan kendali (Kodal). Namun demikian, kompleksitas ancaman cyber warfare menuntut kapabilitas yang lebih dari sekadar pembentukan satuan; TNI membutuhkan interoperabilitas antarmatra, kemampuan respons cepat, sistem deteksi dini, serta doktrin operasional siber yang adaptif dan selaras dengan karakter ancaman kontemporer.

Dalam kerangka itulah, penguatan Satuan Siber TNI menjadi isu strategis bagi negara, mengingat satuan ini berada pada garda terdepan dalam menjaga keamanan sistem komando dan kendali, jaringan komunikasi militer, serta infrastruktur pertahanan digital. Tantangan utama mencakup pembangunan interoperabilitas yang memadai antarmatra TNI, integrasi sistem teknologi informasi dalam operasi gabungan, serta peningkatan kemampuan personel dalam memahami pola ancaman siber lintas domain. Selain itu, strategi penguatan Kodal menjadi elemen penting untuk memastikan bahwa proses pengambilan keputusan dalam menghadapi serangan siber dapat berlangsung cepat, akurat, dan berbasis informasi real-time. Pandangan Lewin (1947) mengenai pentingnya penguatan sistemik dalam perubahan organisasi menegaskan

Received: November 19, 2025 – Revised: November 25, 2025 - Accepted: Desember 21, 2025 - Published online: January 30, 2026

bahwa transformasi satuan siber TNI harus dilakukan secara menyeluruh agar hasilnya bersifat berkelanjutan dan melembaga.

Meskipun sejumlah penelitian telah membahas isu keamanan siber nasional dan kebijakan pertahanan digital, kajian yang secara langsung menempatkan Satuan Siber TNI sebagai fokus analisis masih terbatas. Penelitian sebelumnya banyak berfokus pada aspek regulasi, kebijakan keamanan informasi, atau studi ancaman siber secara umum tanpa secara spesifik menelaah penguatan satuan militer di domain siber, efektivitas interoperabilitas antarmatra, serta strategi Kodal di dalam operasi pertahanan siber. Oleh karena itu, penelitian ini memiliki kebaruan (novelty) dengan memberikan analisis komprehensif mengenai penguatan Satuan Siber TNI menghadapi cyber warfare melalui tiga aspek utama: (1) peran dan kapabilitas satuan siber dalam strategi pertahanan negara, (2) tingkat interoperabilitas siber antarmatra TNI dalam operasi gabungan, dan (3) strategi penguatan sistem komando dan pengendalian untuk memastikan kecepatan serta efektivitas respons terhadap ancaman siber.

Dengan demikian, penelitian ini tidak hanya memberikan kontribusi teoretis terhadap pengembangan kajian strategi pertahanan siber dalam studi militer, tetapi juga menawarkan rekomendasi praktis bagi pemerintah, Kementerian Pertahanan, dan TNI dalam meningkatkan kesiapan pertahanan digital nasional. Penelitian ini diharapkan dapat menjadi rujukan dalam perumusan kebijakan, pengembangan doktrin, serta pembentukan postur pertahanan siber negara yang adaptif, responsif, dan terintegrasi dalam menghadapi dinamika ancaman cyber warfare yang semakin kompleks.

Metode

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif untuk memahami secara mendalam strategi penguatan Satuan Siber TNI dalam menghadapi ancaman cyber warfare. Pendekatan kualitatif dipilih karena mampu menggali makna, pengalaman, serta perspektif para informan yang terlibat langsung dalam penyelenggaraan pertahanan siber. Sesuai pandangan Creswell (2013), penelitian kualitatif dilakukan dalam konteks alamiah dengan peneliti sebagai instrumen utama, sementara Sugiyono (2017) menekankan bahwa metode ini harus memenuhi prinsip rasional, empiris, dan sistematis. Dengan demikian, peneliti berperan aktif dalam menggali data terkait kebijakan, struktur organisasi, serta kesiapan operasional Satuan Siber TNI.

Desain penelitian bersifat deskriptif kualitatif, dengan sumber data primer dan sekunder. Data primer diperoleh melalui wawancara mendalam kepada pejabat Satuan Siber TNI (AD, AL, dan AU), pejabat teknis Kementerian Pertahanan, serta perwakilan Badan Siber dan Sandi Negara (BSSN). Wawancara dilakukan secara terstruktur dengan pedoman pertanyaan, namun tetap memberikan ruang eksploratif untuk memperkaya informasi. Data sekunder diperoleh melalui studi literatur terhadap dokumen resmi pemerintah, regulasi pertahanan siber, laporan kebijakan, buku, jurnal ilmiah, serta publikasi lain yang relevan dengan fokus penelitian.

Pemilihan informan dilakukan dengan teknik purposive sampling, yakni pemilihan subjek berdasarkan kompetensi dan relevansi dengan isu penelitian. Informan merupakan pejabat yang memiliki pengetahuan, pengalaman operasional, dan kewenangan dalam penyelenggaraan pertahanan siber, terdiri dari A1 (Dansatkal Satsiber TNI), A2 (Dansatlak Kalsi Pussiberad), A3 (Kasiops Satsiber Dispamsanau), dan A4 (Kepala Satsiberal). Proses pengumpulan data juga dilengkapi dengan observasi tidak terstruktur terhadap mekanisme kerja dan pola koordinasi Satuan Siber TNI, serta studi

Received: November 19, 2025 – Revised: November 25, 2025 - Accepted: Desember 21, 2025 - Published online: January 30, 2026

dokumentasi terhadap regulasi dan laporan kebijakan pertahanan siber.

Analisis data dilakukan menggunakan model Miles dan Huberman (1994), yang meliputi tahap reduksi data, penyajian data, dan penarikan kesimpulan. Reduksi data dilakukan dengan memilah informasi penting sesuai fokus penelitian, penyajian data disusun dalam bentuk narasi tematik, sedangkan kesimpulan diperoleh melalui interpretasi dan penguatan pola hubungan antar-temuan. Untuk menjamin validitas data, penelitian menerapkan triangulasi sumber dan metode dengan membandingkan informasi dari wawancara, observasi, dan dokumentasi. Aspek keabsahan data dijamin melalui empat kriteria: kredibilitas, transferabilitas, dependabilitas, dan konfirmabilitas sesuai standar penelitian kualitatif.

Penelitian dilaksanakan pada tahun 2025 di beberapa lokasi yang berperan penting dalam sistem pertahanan siber nasional, yaitu Satuan Siber TNI dan Badan Siber dan Sandi Negara (BSSN). Fokus penelitian diarahkan pada tiga variabel utama, yaitu peran Satuan Siber TNI dalam menghadapi cyber warfare, tingkat interoperabilitas antarmatra dalam operasi siber, serta strategi penguatan sistem komando dan pengendalian (Kodal).

Hasil dan Pembahasan

Peran Satuan Siber TNI dalam Strategi Pertahanan Negara Menghadapi Cyber Warfare

Penelitian mengungkap bahwa perkembangan inovasi teknologi siber menjadi faktor utama dalam memperkuat strategi pertahanan negara. Teknologi seperti sistem keamanan digital, pusat operasi siber, jaringan komunikasi terenkripsi, intrusion detection system, threat intelligence platform, dan pemantauan berbasis kecerdasan buatan mempercepat kemampuan TNI dalam mendeteksi, menganalisis, dan merespons ancaman cyber warfare. Peningkatan kapabilitas ini meningkatkan perlindungan terhadap infrastruktur strategis nasional sekaligus memperkuat daya tangkal di ranah non-fisik.

Penguasaan teknologi oleh Satuan Siber TNI menunjukkan kontribusi langsung terhadap peningkatan ketahanan strategis nasional, sesuai konsep Pertahanan Negara yang menempatkan ruang siber sebagai domain baru kedaulatan. Proses penguatan ini menuntut penyesuaian struktur organisasi, penguatan kapasitas sumber daya manusia, dan pembaruan kebijakan pertahanan agar dapat mengimbangi dinamika perubahan ancaman digital.

Peran Satuan Siber TNI dalam konteks Cyberpower Theory tercermin melalui pembangunan kemampuan cyber defense dan cyber intelligence yang mampu menciptakan efek penangkalan. Penguatan ini meningkatkan posisi strategis Indonesia dalam menjaga stabilitas kawasan. Efektivitas kekuatan siber ditemukan sangat dipengaruhi oleh koordinasi nasional dengan BSSN dan Kementerian Pertahanan. Proses transformasi yang terjadi sejalan dengan konsep Revolution in Military Affairs (RMA). Penerapan komputasi, enkripsi, otomasi sistem komando, dan integrasi kemampuan elektronik serta informasi mengubah pola peperangan menuju dominasi informasi. Transformasi ini menuntut reformasi doktrin, strategi, dan pelatihan pertahanan negara, serta kebutuhan investasi pada infrastruktur digital.

Implementasi penguatan Satuan Siber TNI memperlihatkan integrasi teknologi, doktrin, dan sumber daya manusia sebagai satu kesatuan. Ketiga elemen ini menjadi penentu keberhasilan modernisasi pertahanan siber dan kesiapan negara menghadapi eskalasi ancaman di era perang informasi.

Received: November 19, 2025 – Revised: November 25, 2025 - Accepted: Desember 21, 2025 - Published online: January 30, 2026

Tingkat Interoperabilitas Antar Matra TNI dalam Operasi Pertahanan Siber

Interoperabilitas antar matra TNI muncul sebagai elemen strategis yang menentukan efektivitas pertahanan siber nasional. Integrasi sistem, prosedur, dan jaringan informasi antar matra menggambarkan kesiapan TNI menghadapi ancaman yang bersifat multidomain dan asimetris. Interoperabilitas siber mendukung implementasi postur pertahanan adaptif yang memadukan dunia fisik dan digital.

Kekuatan interoperabilitas berpengaruh pada kemampuan pertahanan untuk mengendalikan dan mengintegrasikan informasi sebagaimana dijelaskan dalam Cyberpower Theory. Satuan Siber TNI menjadi simpul penting melalui komunikasi terenkripsi, joint cyber operation center, dan mekanisme pertukaran data aman. Integrasi informasi ini meningkatkan kesiapan menghadapi serangan siber kompleks.

Teori Interoperabilitas tercermin dalam kebutuhan keseragaman doktrin, kompatibilitas sistem, dan sinkronisasi prosedur antarmatra. Standardisasi jaringan komunikasi, protokol keamanan terpadu, dan latihan gabungan menjadi komponen yang ditemukan sangat mempengaruhi keberhasilan operasi siber. Penelitian menemukan tantangan berupa ketidaksinkronan infrastruktur komunikasi, keterbatasan kapasitas teknis personel, serta keragaman perangkat antarmatra. Tantangan ini menghambat kelancaran real-time data sharing dan efektivitas respons simultan.

Arah transformasi pertahanan menuju konsep network-centric operations sejalan dengan Revolution in Military Affairs (RMA). Integrasi battle management system, cyber situational awareness platform, dan sistem operasi digital meningkatkan presisi dan simultanitas operasi gabungan. Interoperabilitas berperan langsung dalam memperkuat sistem Komando dan Pengendalian (C2). Integrasi C2 antar matra mempercepat keputusan strategis, meminimalkan tumpang tindih perintah, dan meningkatkan respons kolektif terhadap ancaman digital.

Penelitian menunjukkan bahwa tingkat interoperabilitas antar matra meningkat dan berada pada arah positif, meskipun masih membutuhkan peningkatan modernisasi sistem, pelatihan bersama, dan kebijakan keamanan siber di seluruh tingkat komando..

Strategi Penguatan Sistem Komando dan Pengendalian (C2) dalam Menghadapi Ancaman Siber

Penguatan sistem Komando dan Pengendalian (C2) menjadi elemen utama dalam menghadapi ancaman siber yang semakin kompleks. Sistem C2 berfungsi sebagai pusat keputusan strategis yang menghubungkan seluruh matra melalui rantai komando digital yang solid. Integrasi C2 mendukung kecepatan reaksi dan kesatuan arah perintah dalam operasi pertahanan siber nasional.

Dalam kerangka Cyberpower Theory, C2 digital menjadi instrumen kekuasaan negara untuk mempertahankan kontrol terhadap domain siber. Kemampuan C2 yang kuat menciptakan decision superiority dengan menyediakan data intelijen real-time bagi pengambilan keputusan cepat dan akurat. Sistem ini memperkuat daya tangkal dan menjaga kedaulatan informasi negara.

Efektivitas C2 sangat bergantung pada interoperabilitas lintas matra. Integrasi sistem informasi, komunikasi, serta sensor digital memastikan perintah dari pusat komando dapat segera diimplementasikan di seluruh tingkat operasi. Pembangunan Cyber Operation Command Center menjadi temuan penting yang memperlihatkan arah transformasi C2 TNI. Transformasi C2 yang diamati mencerminkan implementasi nyata

Received: November 19, 2025 – Revised: November 25, 2025 - Accepted: Desember 21, 2025 - Published online: January 30, 2026

RMA. Penerapan AI, machine learning, dan sistem pemantauan otomatis meningkatkan kemampuan prediksi ancaman dan respons proaktif. Sistem ini memperluas kemampuan pengendalian operasi multidomain.

Penguatan C2 memerlukan kecepatan keputusan, keamanan jaringan komunikasi, distribusi perintah yang efektif, dan kesiapan operator. Penelitian menemukan bahwa peningkatan kompetensi personel siber dan penguatan sistem cadangan menjadi kebutuhan penting untuk menjaga kesinambungan komando saat terjadi gangguan.

Penerapan C2 digital memperkuat unity of command di seluruh lapisan pertahanan, menghubungkan operasi siber dengan operasi konvensional melalui joint command framework. Integrasi ini meningkatkan efisiensi, presisi, dan efektivitas keseluruhan operasi pertahanan nasional.

Kesimpulan

Penelitian ini menyimpulkan bahwa penguatan Satuan Siber TNI merupakan imperatif strategis dalam membangun postur pertahanan negara yang adaptif terhadap dinamika cyber warfare, dan tidak semata-mata dipandang sebagai kebutuhan teknis. Satuan Siber TNI berperan sentral sebagai garda terdepan dalam menjaga kedaulatan digital nasional melalui perluasan spektrum pertahanan dari ranah konvensional ke ranah non-konvensional, yang diwujudkan melalui sistem pengawasan terintegrasi, kemampuan deteksi dini, serta perlindungan infrastruktur informasi vital pertahanan negara.

Hasil penelitian juga menunjukkan bahwa tingkat interoperabilitas antar matra mengalami perkembangan positif seiring penerapan sistem C4ISR dan pelaksanaan latihan gabungan secara berkelanjutan. Namun demikian, masih terdapat tantangan signifikan berupa disparitas protokol keamanan dan ketergantungan terhadap teknologi asing, yang berpotensi menghambat efektivitas integrasi komando siber. Oleh karena itu, harmonisasi sistem berbasis teknologi domestik serta standardisasi Standard Operating Procedure (SOP) menjadi faktor krusial dalam mengoptimalkan integrasi dan sinergi pertahanan siber antar matra TNI.

Lebih lanjut, penguatan sistem Komando dan Pengendalian (C2) perlu diarahkan pada digitalisasi menyeluruh jaringan komando dan adopsi teknologi prediktif berbasis kecerdasan buatan (AI-driven decision support system). Transformasi ini penting untuk menjamin kecepatan pengambilan keputusan (speed of command) dan keseragaman kesadaran situasional (situational awareness) secara real-time, sehingga respons terhadap ancaman dan insiden siber dapat dilaksanakan secara presisi dan terkoordinasi. Secara keseluruhan, transformasi Satuan Siber TNI merepresentasikan evolusi pertahanan Indonesia menuju kemandirian teknologi dan keunggulan informasi (information dominance), yang menjadi determinan utama dalam menjaga stabilitas keamanan nasional di era peperangan modern.

Saran

Berdasarkan kesimpulan penelitian mengenai peran dan kesiapan Satuan Siber TNI, penelitian ini mengajukan beberapa rekomendasi strategis kepada para pemangku kepentingan terkait guna memperkuat sistem pertahanan siber nasional secara komprehensif.

Pertama, bagi Pemerintah Indonesia, diperlukan penyusunan regulasi nasional terpadu yang mampu mengintegrasikan seluruh komponen pertahanan digital, termasuk TNI, Badan Siber dan Sandi Negara (BSSN), serta industri pertahanan

Received: November 19, 2025 – Revised: November 25, 2025 - Accepted: Desember 21, 2025 - Published online: January 30, 2026

nasional. Regulasi tersebut perlu didukung oleh peningkatan alokasi anggaran khusus bagi riset, pengembangan, dan inovasi teknologi pertahanan siber guna mengurangi ketergantungan terhadap produk dan perangkat asing, sekaligus mendorong kemandirian industri pertahanan dalam negeri.

Kedua, bagi Kementerian Pertahanan, disarankan untuk menyusun Cyber Defense Roadmap jangka panjang yang berorientasi pada pengembangan kemampuan pertahanan siber berbasis teknologi mutakhir, seperti kecerdasan buatan (Artificial Intelligence). Selain itu, Kementerian Pertahanan perlu memprioritaskan standardisasi doktrin dan sistem C4ISR di seluruh matra TNI guna mencegah tumpang tindih kebijakan, meningkatkan efektivitas integrasi komando, serta mempercepat alih teknologi melalui kerja sama internasional yang bersifat selektif dan strategis.

Ketiga, bagi Tentara Nasional Indonesia, penguatan Satuan Siber perlu difokuskan pada tiga aspek utama. Pertama, penguatan sumber daya manusia melalui kewajiban sertifikasi berstandar internasional bagi personel siber serta penerapan sistem rotasi penugasan berbasis kompetensi untuk menutup kesenjangan keahlian teknis. Kedua, peningkatan interoperabilitas antar matra melalui intensifikasi latihan gabungan siber dengan skenario serangan real-time guna menguji keandalan prosedur operasi gabungan. Ketiga, modernisasi sistem Komando dan Pengendalian (C2) dengan mengembangkan Cyber Command Center sebagai pusat kendali terintegrasi yang mampu melakukan respons prediktif terhadap anomali jaringan, sehingga penanganan ancaman siber tidak hanya bersifat reaktif, tetapi juga preventif dan adaptif.

Daftar Pustaka

Antara News. (2022, Agustus 15). Situs resmi TNI AD diretas kelompok Indian Cyber Mafia. Diakses dari https://www.antaranews.com

CNN Indonesia. (2017, April 28). Situs Telkomsel diretas, muncul protes tarif internet. Diakses dari https://www.cnnindonesia.com

Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Hipdizah, S. A., Purwanto, S., Hendarwoto, Y., Duarte, R. F., Siagian, F., & Han, M. (2025). Buku ajar doktrin militer. Jakarta: Yayasan Putra Adi Dharma.

Kementerian Pertahanan Republik Indonesia. (2007). Doktrin pertahanan negara. Jakarta: Departemen Pertahanan Republik Indonesia.

Kementerian Pertahanan Republik Indonesia. (2017). Peraturan Menteri Pertahanan Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara. Jakarta: Kementerian Pertahanan Republik Indonesia.

Kompas. (2013, Januari 28). Anonymous Indonesia retas puluhan situs pemerintah. Diakses dari https://www.kompas.com

Kompas. (2016, November 10). Bank Indonesia sebut serangan siber meningkat signifikan. Diakses dari https://www.kompas.com

Kusumaatmadja, M. (1993). Hukum internasional dan keamanan nasional. Bandung: Alumni.

Lewin, K. (1947). Frontiers in group dynamics: Concept, method and reality in social science; social equilibria and social change. Human Relations, 1(1), 5–41.

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). Thousand Oaks, CA: SAGE Publications.

Purwanto, S., Purnomo, M. R., & Budiman, H. (2025). Power dynamics in decision making: A qualitative analysis. POWER, 2(1), 80–86.

Sugiyono. (2017). Metode penelitian kuantitatif, kualitatif, dan R&D. Bandung: Alfabeta.

Received: November 19, 2025 – Revised: November 25, 2025 - Accepted: Desember 21, 2025 - Published online: January 30, 2026