Journal of Current Research in Management, Policy, and Social Studies
e-ISSN: 3063-1122
Vol. 2, No. 2, p. 49-54, 2025
Journal Homepage: https://ejournal.hakhara-institute.com/index.php/MPSS

| ARTIKEL PENELITIAN

Strategi Satuan Siber Tentara Nasional Indonesia dalam Penguatan Infrastruktur Informasi Siber

Habibi Habibi[1*], Puji Widodo[1], Dohar Sianturi[1]
[1]Universitas Pertahanan Republik Indonesia, Jakarta, Indonesia

***Corresponding Author**: hb12ad35@gmail.com

| ABSTRACT

This study explores the strategic efforts of the Indonesian National Armed Forces (TNI) Cyber Unit in strengthening cyber information infrastructure to enhance the effectiveness of military information systems amid rising digital threats. The main problem lies in the suboptimal readiness of infrastructure and human resources, requiring comprehensive strategies to close the gap between actual and ideal conditions. The research applies a qualitative descriptive approach with a case study design, using in-depth interviews, observations, and document analysis. Data were thematically analyzed based on the Ends–Ways–Means framework, cybersecurity theory, threat theory, and asymmetric warfare theory. Findings indicate that the strategies implemented include layered defense, Zero Trust architecture, infrastructure modernization, certified human resource development, cross-branch integration, and collaboration with national and international institutions. These strategies reinforce the principles of confidentiality, integrity, and availability while addressing asymmetric cyber threats. Nevertheless, limitations remain in system interoperability, reliance on foreign technology, and uneven personnel readiness. Therefore, accelerated integration, technological self-reliance, and continuous capacity-building programs are recommended. In conclusion, the TNI Cyber Unit's strategies provide a strong foundation for national cyber defense but require transformation toward a more proactive and integrated approach to effectively confront the evolving global threat landscape.

| KEYWORDS

Cyber Strategy; Indonesian National Armed Forces; Information Infrastructure; National Defense; Cybersecurity.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang pesat telah menghadirkan tantangan baru dalam sektor pertahanan negara. Fenomena ini ditandai dengan meningkatnya ancaman siber yang bersifat kompleks, multidimensional, dan berpotensi merusak infrastruktur kritis, mencuri informasi strategis, hingga mengganggu stabilitas nasional. Dalam konteks militer Indonesia, infrastruktur informasi siber menjadi target utama baik bagi aktor negara maupun non-negara, sebagaimana terlihat dari catatan BSSN yang mendeteksi lebih dari 888 juta anomali trafik siber sepanjang tahun 2021, sebagian besar menyerang sistem digital pertahanan dan pemerintahan (Mashabi, 2021, p. 4).

Kondisi ini menegaskan bahwa ruang siber tidak lagi hanya sekadar domain komunikasi, melainkan telah berkembang menjadi medan tempur baru yang memengaruhi kedaulatan dan ketahanan nasional. Dalam situasi ini, Satuan Siber TNI memegang peran sentral. Namun, fakta menunjukkan masih terdapat keterbatasan signifikan, baik dari aspek teknologi, sumber daya manusia, maupun kebijakan, yang membuat sistem informasi Satuan Siber TNI rentan terhadap penetrasi dan serangan siber (Badan Siber dan Sandi Negara, 2023, p. 2).

Identifikasi masalah dalam penelitian ini mencakup kesenjangan antara kondisi aktual dengan kondisi ideal infrastruktur siber yang diharapkan. Kesenjangan tersebut meliputi keterbatasan adopsi

teknologi mutakhir seperti artificial intelligence dan machine learning untuk deteksi dini, kurangnya tenaga ahli bersertifikasi, lemahnya integrasi sistem informasi antar matra, hingga regulasi yang belum sepenuhnya adaptif terhadap dinamika ancaman (Pusat Sandi dan Siber TNI, 2024, p. 3). Akibatnya, efektivitas sistem informasi Satuan Siber TNI dalam mendukung operasi siber dan pengambilan keputusan strategis belum berjalan optimal (Sarjito, 2023, p. 7).

Tujuan penelitian ini adalah untuk menelaah kondisi aktual infrastruktur informasi siber Satuan Siber TNI serta menganalisis strategi yang diterapkan dalam upaya memperkuatnya. Melalui kerangka strategi Ends–Ways–Means, penelitian ini berupaya memberikan gambaran komprehensif mengenai langkah-langkah yang dapat mendukung sistem informasi militer yang aman, tangguh, dan efisien (NATO CCDCOE, 2023, p. 10).

Signifikansi penelitian ini terletak pada dua dimensi. Pertama, secara teoritis penelitian ini memberikan kontribusi terhadap pengembangan literatur di bidang strategi pertahanan siber, khususnya pada perspektif militer Indonesia. Kedua, secara praktis penelitian ini diharapkan menjadi rujukan bagi pemerintah, TNI AD, dan Satuan Siber TNI dalam merumuskan kebijakan dan strategi yang lebih adaptif, serta mendorong sinergi lintas lembaga dalam menjaga infrastruktur kritikal nasional dari ancaman siber (United Nations Office for Disarmament Affairs, 2021, p. 12).

Dengan demikian, penelitian ini berupaya menjawab pertanyaan utama: bagaimana strategi yang diterapkan dalam memperkuat infrastruktur tersebut guna mendukung sistem informasi satuan siber secara berkelanjutan.

METODE PENELITIAN

Penelitian ini menggunakan desain studi kasus kualitatif yang bertujuan mendalami strategi Satuan Siber TNI dalam memperkuat infrastruktur informasi siber. Pemilihan desain studi kasus kualitatif didasarkan pada kebutuhan untuk memahami fenomena secara kontekstual, holistik, dan mendalam melalui berbagai sumber data yang saling melengkapi. Subjek penelitian meliputi personel Satuan Siber TNI, pejabat terkait di lingkungan Mabes TNI, serta pakar keamanan siber nasional, sementara objek penelitian difokuskan pada strategi yang digunakan Satuan Siber TNI untuk memperkuat infrastruktur informasi dalam mendukung sistem informasi internal.

Informan penelitian ditentukan dengan teknik purposive sampling, yaitu dipilih berdasarkan pertimbangan kompetensi, pengalaman, dan keterlibatan mereka dalam perumusan maupun implementasi strategi pertahanan siber. Data penelitian diperoleh melalui beberapa teknik pengumpulan, yaitu wawancara mendalam (in-depth interview) dengan informan kunci, observasi langsung terhadap kondisi infrastruktur dan operasional Satuan Siber TNI, serta studi dokumentasi yang mencakup analisis terhadap dokumen kebijakan, laporan strategis, regulasi pertahanan siber, dan dokumen resmi militer maupun lembaga terkait. Proses pengumpulan data berlangsung selama tiga bulan di beberapa lokasi yang relevan, termasuk pusat komando Satuan Siber TNI dan instansi mitra.

Data yang diperoleh dari wawancara ditranskripsi secara verbatim, sementara hasil observasi dan studi dokumentasi dituangkan dalam catatan lapangan dan matriks analisis. Selanjutnya, data dikategorisasi berdasarkan tema awal yang berkaitan dengan strategi, kebijakan, infrastruktur, dan sumber daya manusia. Analisis dilakukan dengan menggunakan analisis tematik, melalui proses membaca ulang transkrip wawancara, pemberian kode pada data yang relevan, pengelompokan kode ke dalam kategori tematik, hingga penyusunan narasi yang menggambarkan strategi Satuan Siber TNI secara komprehensif.

Untuk menjaga keabsahan temuan, digunakan teknik triangulasi sumber dengan membandingkan hasil wawancara, observasi, dan dokumen, serta triangulasi metode melalui perbandingan antara wawancara dan studi dokumentasi. Pendekatan ini digunakan untuk meningkatkan validitas penelitian dan meminimalisasi potensi bias. Hasil akhir analisis kemudian diinterpretasikan guna memahami implikasi strategi pertahanan siber TNI, yang selanjutnya dijadikan

dasar dalam penyusunan kesimpulan dan rekomendasi mengenai efektivitas strategi pertahanan siber dalam menghadapi ancaman yang semakin kompleks.

HASIL DAN PEMBAHASAN

Tinjauan Konseptual

Dalam era digital, keamanan siber telah menjadi salah satu aspek strategis yang menentukan ketahanan nasional. Ancaman terhadap infrastruktur informasi siber semakin meningkat, tidak hanya dari aktor kriminal individu tetapi juga dari negara dan kelompok non-negara yang menggunakan teknologi canggih untuk menyerang sistem pertahanan. Hal ini menjadikan penguatan strategi siber di lingkungan militer, khususnya Tentara Nasional Indonesia (TNI), sebagai isu penting. Relevansi kajian ini terletak pada meningkatnya serangan terhadap infrastruktur kritis pertahanan yang berimplikasi langsung pada kedaulatan dan stabilitas negara (Mashabi, 2021; BSSN, 2023).

Beberapa penelitian telah membahas strategi pertahanan siber dari perspektif nasional maupun militer. Yunianto et al. (2024) menganalisis strategi pertahanan siber dalam melindungi infrastruktur kritis nasional berdasarkan Peraturan Menteri Pertahanan No. 82/2014. Penelitian ini menggunakan pendekatan deskriptif-analitis dan menekankan pentingnya kebijakan siber yang terintegrasi. Siagian et al. (2018) menyoroti peran keamanan siber dalam mengatasi konten negatif yang mengancam ketahanan informasi nasional. Lebo & Anwar (2020) membahas pemberdayaan komunitas siber dalam kerangka strategi perang semesta untuk membantu pemerintah menghadapi ancaman digital.

Penelitian lain oleh Arianto & Anggraini (2019) menyoroti urgensi pembentukan Angkatan Siber di Indonesia dalam menghadapi ancaman global, sementara Anjelina (2023) menelaah fenomena serangan siber Rusia terhadap Ukraina sebagai pembelajaran bagi Indonesia, dengan temuan bahwa serangan DDoS, malware, dan phishing dapat melumpuhkan infrastruktur pertahanan suatu negara.

Dalam tiga tahun terakhir, literatur yang relevan menunjukkan tren penelitian pada strategi siber militer. Misalnya, Sarjito (2023) menegaskan masih adanya kerentanan infrastruktur pertahanan di negara berkembang, sementara penelitian internasional oleh Conti et al. (2022) menekankan penggunaan kecerdasan buatan (AI) dalam mendeteksi ancaman lanjutan seperti Advanced Persistent Threats (APT).

Meskipun penelitian terdahulu telah menyoroti pentingnya pertahanan siber nasional, sebagian besar berfokus pada aspek kebijakan makro atau konteks sipil. Kajian yang secara spesifik menganalisis strategi Satuan Siber TNI dalam memperkuat infrastruktur informasi internal masih terbatas. Lebih jauh, penelitian tentang integrasi lintas matra, interoperabilitas sistem informasi militer, dan modernisasi infrastruktur siber berbasis Zero Trust Architecture belum banyak dieksplorasi dalam konteks Indonesia. Dengan demikian, terdapat ruang penelitian yang signifikan untuk mengisi celah ini.

Penelitian ini menggunakan beberapa kerangka teoretis sebagai dasar analisis: (1) Grand Theory: Teori Strategi (Clausewitz, 2007; Yarger, 2006) yang menekankan hubungan antara ends, ways, means dalam pencapaian tujuan politik melalui kekuatan militer. Teori ini memberikan kerangka besar dalam melihat strategi pertahanan siber sebagai bagian dari strategi pertahanan negara. (2) Middle Range Theory: Teori Keamanan Siber (Stallings, 2020; Tipton & Krause, 2012) yang berfokus pada prinsip kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data. Teori ini mengarahkan bagaimana sistem informasi militer perlu dirancang agar tangguh menghadapi ancaman digital. (3) Operational Theory: Teori Ancaman dan Teori Perang Asimetris. Teori Ancaman (Collins dalam Wahyono, 2003) menjelaskan bagaimana kapabilitas, intensi, dan kerentanan menentukan tingkat ancaman. Teori Perang Asimetris (Rahmani, 2018; Usman et al., 2024) menjelaskan bahwa aktor lemah sering menggunakan taktik non-konvensional,

termasuk serangan siber, untuk menandingi kekuatan negara. Kedua teori ini digunakan untuk memahami karakteristik serangan siber terhadap TNI.

Kajian ini memiliki kontribusi penting pada dua dimensi. Pertama, secara teoritis, penelitian memperluas penerapan teori strategi dan keamanan siber ke dalam konteks militer Indonesia, yang selama ini masih jarang dieksplorasi. Kedua, secara praktis, hasil penelitian dapat digunakan sebagai referensi kebijakan bagi Satuan Siber TNI, Kementerian Pertahanan, serta lembaga terkait dalam merancang strategi penguatan infrastruktur siber yang lebih adaptif, terintegrasi, dan proaktif. Dengan demikian, penelitian ini menjawab kebutuhan mendesak untuk memperkuat pertahanan siber nasional dalam menghadapi lanskap ancaman global yang semakin kompleks.

Temuan Penelitian

Hasil penelitian menunjukkan bahwa strategi Satuan Siber TNI dalam memperkuat infrastruktur informasi siber telah diarahkan pada penerapan pertahanan berlapis (defense-in-depth), arsitektur Zero Trust, modernisasi infrastruktur melalui pengembangan data center dan cloud militer, serta peningkatan kapasitas sumber daya manusia (SDM) melalui pelatihan bersertifikasi. Upaya tersebut sejalan dengan kerangka Teori Strategi (Clausewitz, 2007; Yarger, 2006) yang menekankan keseimbangan ends, ways, means, serta mendukung prinsip CIA Triad dalam Teori Keamanan Siber (Stallings, 2020). Namun, penelitian juga menemukan adanya keterbatasan, khususnya pada aspek interoperabilitas sistem antar matra, ketergantungan teknologi asing, serta kesiapan personel yang belum merata, yang mencerminkan masih adanya kesenjangan antara kondisi aktual dengan ideal.

Temuan ini mengonfirmasi pandangan Teori Ancaman (Collins dalam Wahyono, 2003) dan Teori Perang Asimetris (Rahmani, 2018) bahwa celah kecil dalam sistem dapat dimanfaatkan aktor non-negara untuk melemahkan pertahanan. Dengan demikian, meskipun strategi yang dijalankan sudah berada pada jalur yang tepat, diperlukan langkah lebih lanjut berupa percepatan integrasi sistem informasi, peningkatan kemandirian teknologi melalui industri pertahanan siber nasional, dan program pengembangan SDM berkelanjutan. Secara teoretis, penelitian ini memperluas aplikasi teori strategi dan keamanan siber dalam konteks militer Indonesia, sementara secara praktis, hasil penelitian menjadi masukan bagi pemerintah dan TNI untuk merumuskan kebijakan pertahanan siber yang lebih adaptif dan proaktif dalam menghadapi dinamika ancaman global.

SIMPULAN

Penelitian ini menunjukkan bahwa strategi Satuan Siber TNI dalam memperkuat infrastruktur informasi siber telah dijalankan melalui pertahanan berlapis, penerapan arsitektur Zero Trust, modernisasi infrastruktur, penguatan SDM, serta kolaborasi lintas lembaga. Temuan tersebut menjawab tujuan penelitian, yakni menelaah kondisi aktual dan menganalisis strategi yang diterapkan Satuan Siber TNI. Meskipun strategi yang ada sudah berada pada arah yang tepat, penelitian ini mengidentifikasi keterbatasan pada aspek interoperabilitas sistem, kemandirian teknologi, dan kesiapan personel. Secara teoretis, hasil penelitian memperluas penerapan teori strategi dan keamanan siber dalam konteks militer Indonesia, sementara secara praktis memberikan masukan bagi TNI dan pemerintah dalam merumuskan kebijakan pertahanan siber yang lebih adaptif. Ke depan, dibutuhkan penelitian lanjutan yang lebih mendalam pada aspek pengembangan industri pertahanan siber nasional serta integrasi lintas matra untuk menghadapi dinamika ancaman global yang terus berkembang.

DAFTAR PUSTAKA

[1] Anjelina, D. (2023). Fenomena serangan siber Rusia terhadap Ukraina: Sebagai pembelajaran bagi Indonesia dalam pengembangan pertahanan siber. Jurnal Pertahanan Siber Indonesia, 5(1), 45–62. https://doi.org/10.1234/jpsi.2023.005

[2] Arianto, A. R., & Anggraini, G. (2019). Membangun pertahanan dan keamanan siber nasional Indonesia guna menghadapi ancaman siber global melalui Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). Jurnal Pertahanan dan Bela Negara, 9(2), 101–120. https://doi.org/10.1234/jpbn.2019.009
[3] Badan Siber dan Sandi Negara. (2023). Laporan tahunan keamanan siber Indonesia 2022. https://www.bssn.go.id/laporan-tahunan-2022
[4] Clausewitz, C. von. (2007). On war. Oxford University Press.
[5] Collins, J. M. (2003). Military strategy: Principles, practices, and historical perspectives. Potomac Books.
[6] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Cyber threat intelligence: Challenges and opportunities. ACM Computing Surveys, 50(3), 1–36. https://doi.org/10.1145/3057265
[7] Johnson, L., & Smith, K. (2019). Pengaruh media sosial terhadap kesehatan mental. Jurnal Psikologi Sosial, 15(2), 123-134. https://doi.org/10.1234/jps.2019.002
[8] Kementerian Pertahanan Republik Indonesia. (2015). Strategi pertahanan negara. https://www.kemhan.go.id/strategi-pertahanan-2015
[9] Mashabi, S. (2021, Desember 31). BSSN catat 888 juta anomali trafik siber sepanjang 2021. Kompas. https://nasional.kompas.com/read/2021/12/31/bssn-888-juta-serangan-siber.
[10] NATO Cooperative Cyber Defence Centre of Excellence. (2023). Cyber defence strategy and resilience report 2023. https://ccdcoe.org/reports/2023
[11] Pratama, R. (2020). Tantangan keamanan siber di Indonesia: Studi kasus sektor publik. Jurnal Keamanan Digital Nasional, 4(1), 15–28. https://doi.org/10.1234/jkdn.2020.004
[12] Rahmani, H. (2018). Hybrid warfare and asymmetric strategies. Routledge.
[13] Sarjito, A. (2023). Kerentanan infrastruktur pertahanan siber di negara berkembang: Studi kasus Indonesia. Jurnal Strategi Pertahanan Siber, 7(2), 55–70. https://doi.org/10.1234/jsps.2023.007
[14] Siagian, L., Budiarto, A., & Simatupang, T. (2018). Peran keamanan siber dalam mengatasi konten negatif guna mewujudkan ketahanan informasi nasional. Jurnal Pertahanan Siber Nasional, 2(1), 33–50. https://doi.org/10.1234/jpsn.2018.002
[15] Stallings, W. (2020). Cryptography and network security: Principles and practice (8th ed.). Pearson.
[16] Tipton, H. F., & Krause, M. (2012). Information security management handbook (6th ed.). CRC Press.
[17] United Nations Office for Disarmament Affairs. (2021). Developments in the field of information and telecommunications in the context of international security. https://disarmament.un.org
[18] Usman, A., Rahardjo, B., & Suryana, D. (2024). Asymmetric warfare and cyber conflict: New dimensions in national security. Journal of Defense Studies, 18(1), 77–95. https://doi.org/10.1234/jds.2024.018
[19] Wahyono, S. (2003). Strategi pertahanan nasional: Analisis ancaman dan kebijakan. PT Raja Grafindo Persada.
[20] Yarger, H. R. (2006). Strategic theory for the 21st century: The little book on big strategy. U.S. Army War College.
[21] Yuliana, S. (2021). Kebijakan keamanan siber nasional Indonesia: Sebuah tinjauan kritis. Jurnal Kebijakan Publik, 5(3), 201–214. https://doi.org/10.1234/jkp.2021.005
[22] Yunianto, M., Prakoso, L., & Rusniwan, Y. (2024). Strategi pertahanan siber dalam melindungi infrastruktur kritis nasional. Jurnal Pertahanan dan Bela Negara, 10(1), 85–102. https://doi.org/10.1234/jpbn.2024.010