Analisis Pengamanan Markas Komando Korps Marinir dalam Menghadapi Ancaman Sabotase dan Spionase di Era Digital

Bambang Tri Nugroho Saputro*[1], Agus Prabowo Adi[2], Mohammad Jakfarrosi[3]
[1.2.3]Sekolah Staf dan Komando Angkatan Laut, Indonesia
E-mail: bang3tri3@gmail.com

Article Info
Article History
Received: 2026-02-05
Revised: 2026-03-10
Published: 2026-04-14

Keywords:
Marine Corps;
Headquarters;
Security;
Sabotage;
Espionage;
Digital Era;
Layered System.

Abstract
The development of information and communication technology has introduced new challenges to Indonesia's national security, particularly in the form of digital sabotage and espionage targeting strategic military installations. The Marine Corps Headquarters serves as a critical operational decision-making center that is vulnerable to both physical and digital threats. This study aims to analyze the security system of the Marine Corps Headquarters in addressing these threats, evaluate the effectiveness of security procedures, and identify potential vulnerabilities exploitable by external parties. The research employs a qualitative method with a descriptive-analytical approach, combining interviews with security officials, direct observations of the headquarters, and the study of official documents. Analysis was conducted using a security strategy framework and SWOT method to evaluate the strengths, weaknesses, opportunities, and threats affecting the security system. The findings indicate that the headquarters has implemented a layered security system encompassing personnel security, physical security, standard operating procedures, and digital security, which is effective against physical threats. However, integration between physical and digital security requires improvement, personnel capacity in operating digital systems is limited, and integration of legacy and modern technology remains suboptimal, leaving potential security gaps. Based on these findings, the study recommends enhancing system integration, providing continuous cyber training, upgrading technology, and adjusting SOPs based on digital risk assessment to ensure adaptive and sustainable security effectiveness.

Artikel Info
Sejarah Artikel
Diterima: 2026-02-05
Direvisi: 2026-03-10
Dipublikasi: 2026-04-14

Kata kunci:
Korps Marinir;
Markas Komando;
Pengamanan;
Sabotase;
Spionase;
Era Digital;
Sistem Berlapis.

Abstrak
Perkembangan teknologi informasi dan komunikasi membawa tantangan baru bagi keamanan nasional Indonesia, terutama dalam bentuk ancaman sabotase dan spionase digital yang menargetkan instalasi strategis militer. Markas Komando Korps Marinir sebagai pusat pengambilan keputusan operasional menjadi salah satu titik kritis yang rentan terhadap gangguan digital maupun fisik. Penelitian ini bertujuan menganalisis sistem pengamanan Markas Komando Korps Marinir dalam menghadapi ancaman tersebut, menilai efektivitas prosedur pengamanan, serta mengidentifikasi potensi kerawanan yang dapat dimanfaatkan pihak eksternal. Penelitian menggunakan metode kualitatif dengan pendekatan deskriptif analitis, memadukan wawancara dengan pejabat pengamanan, observasi langsung kondisi markas, dan studi dokumen resmi. Analisis dilakukan menggunakan kerangka strategi keamanan dan metode SWOT untuk mengevaluasi kekuatan, kelemahan, peluang, dan ancaman yang memengaruhi sistem pengamanan. Hasil penelitian menunjukkan bahwa pengamanan Markas Komando telah menerapkan sistem berlapis yang mencakup pengamanan personel, pengamanan fisik, prosedur dan kebijakan, serta pengamanan digital, yang efektif untuk menghadapi ancaman fisik. Namun, integrasi antara pengamanan fisik dan digital masih perlu diperkuat, kapasitas personel dalam mengoperasikan sistem digital terbatas, dan integrasi teknologi lama dan baru belum optimal, sehingga membuka celah keamanan potensial. Penelitian ini merekomendasikan peningkatan integrasi sistem, pelatihan siber berkelanjutan, pembaruan teknologi, dan penyesuaian SOP berbasis risiko digital untuk menjamin efektivitas pengamanan yang adaptif dan berkelanjutan.

I. PENDAHULUAN

Lingkungan strategis global dan regional saat ini menunjukkan kompleksitas yang terus meningkat, dipicu oleh rivalitas geopolitik, percepatan kemajuan teknologi informasi, dan munculnya ancaman non-konvensional berbasis siber dan digital (Andrade, 2025). Ancaman tersebut tidak lagi sekadar agresi militer terbuka, melainkan berwujud operasi intelijen, sabotase, dan spionase yang menargetkan instalasi

strategis serta sistem informasi pertahanan negara (Bilqis, 2025). Transformasi ancaman ini menuntut adaptasi strategi keamanan yang mampu menghadapi risiko fisik dan digital secara simultan.

Indonesia, sebagai negara kepulauan dengan posisi strategis di kawasan Indo-Pasifik, menghadapi potensi ancaman yang signifikan terhadap stabilitas nasional, khususnya di wilayah maritim. Dalam konteks tersebut, Korps Marinir sebagai unsur tempur TNI Angkatan Laut memegang peran sentral. Korps ini tidak hanya menjaga kedaulatan wilayah pesisir dan pulau terluar, tetapi juga mendukung pelaksanaan Operasi Militer Perang maupun Operasi Militer Selain Perang. Undang-Undang Nomor 3 Tahun 2025 menegaskan bahwa tugas pokok TNI adalah menegakkan kedaulatan negara, mempertahankan keutuhan wilayah, dan melindungi bangsa dari segala bentuk ancaman (*Undang-Undang Nomor 3 Tahun 2025 tentang Tentara Nasional Indonesia Pasal 7*, 2025).

Perkembangan teknologi digital telah mengubah lanskap ancaman terhadap keamanan nasional (Libicki, 2009). Sabotase dan spionase kini dapat dilakukan tanpa kontak fisik, memanfaatkan kerentanan pada perangkat, jaringan, dan sistem informasi militer (Kaplan, 2016). Teknologi yang sebelumnya meningkatkan efisiensi operasional juga membuka risiko baru terhadap keamanan data strategis, yang menjadi tulang punggung pengambilan keputusan dan keberhasilan operasi militer. Markas Komando Korps Marinir, sebagai pusat pengambilan keputusan strategis, menjadi target utama ancaman tersebut. Insiden sabotase digital pada akhir Agustus 2025, yang menyebabkan perubahan otomatis pada running text di area markas, serta praktik spionase terhadap komunikasi personel, memperlihatkan betapa nyata dan cepatnya risiko digital dapat memengaruhi efektivitas pertahanan (Singer and Friedman, 2014).

Kondisi ini menegaskan bahwa pengamanan markas harus bersifat terintegrasi, menggabungkan proteksi fisik melalui penjagaan gerbang dan sistem pengawasan dengan proteksi digital yang meliputi *firewall,* enkripsi, dan deteksi intrusi. Penelitian ini dirancang untuk menganalisis sistem pengamanan yang diterapkan, mengevaluasi efektivitasnya dalam menghadapi ancaman sabotase dan spionase digital, serta menyusun rekomendasi strategis untuk memperkuat perlindungan markas. Dengan pengamanan yang optimal, Korps Marinir dapat menjalankan tugas pokok TNI secara efektif, memastikan kedaulatan negara tetap terjaga, dan memperkuat stabilitas nasional di tengah tantangan keamanan yang semakin kompleks (Omand, Bartlett and Miller, 2012).

II. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif analitis untuk memahami secara mendalam sistem pengamanan Markas Komando Korps Marinir dalam menghadapi ancaman sabotase dan spionase di era digital (Creswell, 2018). Pendekatan ini memungkinkan penggambaran kondisi aktual pengamanan, mulai dari aspek personel, sarana dan prasarana, prosedur, hingga pemanfaatan teknologi, sekaligus menilai efektivitas dan potensi kerawanan yang mungkin dimanfaatkan pihak yang berniat merusak. Strategi keamanan dijadikan kerangka analisis untuk menelaah faktor internal dan eksternal yang memengaruhi sistem pengamanan, dengan metode SWOT digunakan untuk merumuskan strategi yang adaptif dan tepat sasaran. Unit analisis mencakup pengamanan personel, fisik, informasi dan sistem digital, prosedur serta kebijakan, pemanfaatan teknologi, dan mekanisme koordinasi, sementara data diperoleh melalui wawancara, observasi langsung, dokumentasi resmi, SOP, arsip, dan literatur relevan, semuanya bersifat kualitatif dan deskriptif.

Pengolahan dan analisis data dilakukan secara sistematis melalui pemeriksaan, klasifikasi, reduksi, penyajian naratif, serta penarikan kesimpulan untuk menggambarkan pola dan hubungan antar-komponen pengamanan (Miles, Huberman and Saldaña, 2020). Analisis SWOT digunakan untuk menilai kekuatan, kelemahan, peluang, dan ancaman, sekaligus merumuskan strategi peningkatan sistem pengamanan markas. Tahapan penelitian meliputi persiapan, pengumpulan data, analisis, hingga penyusunan laporan, dengan tujuan memberikan pemahaman komprehensif mengenai efektivitas pengamanan Markas Komando Korps Marinir sekaligus menghasilkan rekomendasi strategis yang relevan untuk menghadapi ancaman digital yang semakin kompleks dan dinamis.

III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Berdasarkan analisis data yang diperoleh melalui wawancara dengan pejabat pengamanan Korps Marinir, observasi langsung kondisi Markas Komando, dan studi dokumen resmi,

dapat disimpulkan bahwa sistem pengamanan Markas Komando telah diterapkan secara berlapis dan sistematis. Sistem ini mencakup pengamanan personel, pengamanan fisik, prosedur dan kebijakan (SOP), serta pengamanan informasi dan sistem digital. Pengamanan fisik dilaksanakan melalui kontrol akses gerbang, patroli internal, pengawasan CCTV, serta prosedur penjagaan rutin oleh personel yang terlatih, yang terbukti efektif dalam mencegah ancaman fisik langsung terhadap fasilitas strategis.

Pengamanan digital telah diterapkan melalui *firewall*, enkripsi data, dan sistem deteksi intrusi (IDS), yang berfungsi untuk mengantisipasi potensi sabotase dan spionase digital terhadap sistem informasi strategis. Temuan lapangan menunjukkan bahwa teknologi digital ini menjadi elemen kritis dalam menjaga integritas data dan mendukung efektivitas pengambilan keputusan operasional.

Penelitian ini menemukan sejumlah kerentanan signifikan dalam sistem pengamanan. Integrasi antara pengamanan fisik dan digital masih belum optimal, sehingga koordinasi dalam merespons ancaman siber berjalan tidak secepat yang diharapkan. Kapasitas personel dalam pengoperasian sistem digital juga terbatas, yang berdampak pada kecepatan dan ketepatan respon terhadap insiden siber (Union, 2021). Selain itu, integrasi antara sistem lama dan teknologi baru belum sepenuhnya sempurna, sehingga membuka peluang bagi akses tidak sah atau manipulasi data. Insiden manipulasi *running text* LED pada Agustus 2025 menjadi bukti konkret bahwa ancaman digital dapat secara langsung memengaruhi koordinasi operasional dan keamanan informasi di Markas Komando. Sistem pengamanan Markas Komando menunjukkan efektivitas pada aspek fisik, namun perlu dilakukan penguatan integrasi digital, peningkatan kapasitas SDM, dan modernisasi teknologi agar dapat menghadapi ancaman sabotase dan spionase digital secara menyeluruh dan berkelanjutan.

B. Pembahasan

Sistem pengamanan Markas Komando Korps Marinir mengikuti prinsip *Defense in Depth*, di mana pengamanan fisik dan digital bekerja secara berlapis dan saling mendukung untuk menciptakan sistem yang komprehensif dan adaptif (Technology, 2020b). Personel markas telah dilatih untuk menjalankan SOP pengamanan, memonitor akses, dan mengawasi area strategis, sehingga pengamanan fisik terbukti mampu mencegah akses ilegal. Namun, wawancara dan juga observasi menunjukkan bahwa kemampuan personel dalam menghadapi ancaman digital masih perlu ditingkatkan agar dapat mendeteksi dini indikasi sabotase atau spionase digital secara cepat dan tepat.

Pengamanan fisik, meskipun kuat, harus diintegrasikan dengan pengamanan digital karena ancaman modern tidak selalu membutuhkan kontak fisik dan serangan siber dapat menembus sistem tanpa terlihat langsung (Cybersecurity, 2021). Pengamanan digital yang meliputi *firewall,* enkripsi, IDS, dan kontrol akses berperan sebagai lapisan pertahanan utama, tetapi efektivitasnya tergantung pada integrasi *real-time* dengan pengawasan personel dan SOP tanggap darurat (Technology, 2020a). Analisis lebih lanjut menunjukkan bahwa SOP pengamanan fisik dan digital dijalankan secara konsisten, namun beberapa prosedur digital masih bersifat reaktif dan perlu penyesuaian berbasis risiko, sehingga prosedur preventif lebih kuat dapat diterapkan.

Teknologi modern menjadi elemen strategis dalam sistem pengamanan, *firewall*, IDS, dan enkripsi mampu meminimalkan risiko akses tidak sah dan menjaga integritas data strategis, tetapi kapasitas SDM dan integrasi sistem lama dengan baru tetap menjadi tantangan signifikan. Berdasarkan analisis SWOT, kekuatan sistem terletak pada personel terlatih, SOP yang jelas, dan penggunaan teknologi modern, sedangkan kelemahan terdapat pada integrasi fisik, digital dan keterbatasan SDM. Peluang muncul dari pelatihan siber berkelanjutan, pemantauan *real-time*, dan pengembangan SOP berbasis risiko digital, sementara ancaman utama berasal dari pihak eksternal yang memanfaatkan celah digital untuk sabotase atau spionase. Dengan memperkuat integrasi antar lapisan pengamanan, meningkatkan kompetensi personel, memperbarui teknologi, dan menyesuaikan SOP berbasis risiko digital, Markas Komando dapat menghadapi ancaman digital yang semakin kompleks sekaligus menjaga efektivitas operasional Korps Marinir secara berkelanjutan, mempertahankan

kesiapsiagaan, dan mendukung kedaulatan nasional.

Tabel 1. Faktor Internal dan Eksternal SWOT Sistem Pengamanan Markas Komando

No	Komponen	Keterangan
1.	Strengths (Kekuatan)	Personel terlatih, SOP pengamanan fisik jelas, penggunaan teknologi keamanan modern *(firewall*, IDS, enkripsi), koordinasi internal berjalan
2.	Weaknesses (Kelemahan)	Integrasi fisik digital belum sempurna, kapasitas SDM terbatas dalam pengoperasian sistem digital, sistem lama belum sepenuhnya terintegrasi
3.	Opportunities (Peluang)	Pelatihan siber berkelanjutan, implementasi sistem monitoring *real-time,* pengembangan SOP berbasis risiko digital
4.	Threats (Ancaman)	Sabotase digital dan spionase oleh pihak eksternal, peretasan data dan manipulasi informasi, ancaman siber bersifat anonim dan lintas batas

Berdasarkan temuan dan analisis SWOT, beberapa langkah strategis disarankan untuk memperkuat sistem pengamanan Markas Komando Korps Marinir. Pertama, meningkatkan integrasi antara pengamanan fisik dan digital agar deteksi dini dan respons terhadap ancaman dapat berjalan secara simultan. Kedua, meningkatkan kapasitas SDM melalui pelatihan berkelanjutan terkait keamanan siber dan pengoperasian sistem digital, sehingga personel mampu merespons ancaman dengan cepat. Ketiga, memperbarui sistem lama dengan teknologi modern yang mendukung monitoring *real-time*, enkripsi data, dan deteksi intrusi otomatis. Keempat, menyesuaikan SOP dengan ancaman digital terkini, termasuk protokol tanggap darurat terhadap serangan siber dan sabotase digital. Kelima, melakukan evaluasi dan audit berkala untuk menilai efektivitas pengamanan serta mengidentifikasi celah yang masih dapat dimanfaatkan pihak eksternal. Dengan penerapan strategi ini, Markas Komando Korps Marinir diharapkan dapat menghadapi ancaman digital yang semakin kompleks dan menjaga efektivitas operasional secara berkelanjutan.

IV. SIMPULAN DAN SARAN

A. Simpulan

1. Sistem pengamanan Markas Komando Korps Marinir telah diterapkan secara berlapis, mencakup pengamanan personel, pengamanan fisik, prosedSiur dan kebijakan (SOP), serta pengamanan digital, yang secara umum efektif dalam menghadapi ancaman fisik maupun sebagian ancaman digital.
2. Integrasi antara pengamanan fisik dan digital masih menjadi tantangan utama, terutama dalam koordinasi real-time dan pemanfaatan teknologi modern secara optimal, sehingga ada potensi celah keamanan yang dapat dimanfaatkan pihak eksternal.
3. Kapasitas sumber daya manusia dalam pengoperasian sistem digital perlu ditingkatkan agar respons terhadap ancaman siber, termasuk sabotase dan spionase digital, dapat dilakukan dengan cepat dan tepat.
4. Teknologi keamanan modern seperti firewall, enkripsi, dan sistem deteksi intrusi berperan strategis dalam menjaga integritas data dan mendukung efektivitas pengamanan, tetapi keberhasilan implementasinya sangat bergantung pada integrasi dengan SOP dan keterampilan personel.

B. Saran

1. Menyelaraskan pengamanan fisik dan digital melalui prosedur operasi yang terintegrasi untuk meningkatkan deteksi dini dan respons terhadap ancaman secara simultan.
2. Melaksanakan pelatihan berkelanjutan terkait keamanan siber, penggunaan sistem digital, dan protokol tanggap darurat agar personel mampu menghadapi ancaman digital dengan efektif.
3. Memperbarui sistem lama dengan teknologi modern yang mendukung monitoring real-time, enkripsi data, dan deteksi intrusi otomatis untuk meminimalkan celah keamanan.
4. Menyesuaikan SOP pengamanan fisik dan digital berbasis risiko, melakukan simulasi insiden secara berkala, serta mengevaluasi efektivitas sistem pengamanan untuk menghadapi ancaman sabotase dan spionase di era digital.

DAFTAR RUJUKAN

Andrade, T.N. de (2025) 'Cybersecurity in the Digital Era: Geopolitical Impacts and Structural Challenges', *IOSR Journal* [Preprint].

Bilqis, S. (2025) 'Geopolitik Cyber Security: Strategi Menghadapi Ancaman Siber terhadap Keamanan Informasi pada Era Digital', *MIJ UIN Malang* [Preprint].

Creswell, J.W. (2018) *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Edited by 4. Thousand Oaks, CA: SAGE Publications. Available at: https://doi.org/10.4135/9781506335193.

Cybersecurity, E.U.A. for (2021) *Cybersecurity and Physical Security Convergence*. Athens: ENISA.

Kaplan, F. (2016) *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster.

Libicki, M.C. (2009) *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Miles, M.B., Huberman, A.M. and Saldaña, J. (2020) *Qualitative Data Analysis: A Methods Sourcebook*. 4th edn. Thousand Oaks: Sage Publications.

Omand, D., Bartlett, J. and Miller, C. (2012) 'Introducing Social Media Intelligence (SOCMINT)', *Intelligence and National Security*, 27(6), pp. 801–823.

Singer, P.W. and Friedman, A. (2014) *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

Technology, N.I. of S. and (2020a) *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. Gaithersburg: NIST.

Technology, N.I. of S. and (2020b) *Zero Trust Architecture (SP 800-207)*. Gaithersburg: NIST.

Undang-Undang Nomor 3 Tahun 2025 tentang Tentara Nasional Indonesia Pasal 7 (2025). Republik Indonesia.

Union, I.T. (2021) *Global Cybersecurity Index 2020*. Geneva: ITU.