ESDJ: Electronika Sea and Defense Journal
ISSN: (online), (print)
DOI: 10.59447

# PENINGKATAN KEAMANAN SIBER PADA SISTEM KOMUNIKASI TERPADU TNI AL

# ENHANCING CYBERSECURITY IN THE INTEGRATED COMMUNICATION SYSTEM OF THE INDONESIAN NAVY

**Muhammad Ghaly Alghifari[1*], Yulian Wardi[1], Yudi Ruspiantoro[1]**
[1.3]Instansi, Jl. Bumimoro Morokrembangan, Surabaya, Jawa Timur, 60178, Indonesia
[2] Instansi, Jl. Semarang No. 5 Malang, Jawa Timur, 65341, Indonesia

*Penulis korespondensi, Surel: wardi.yulian@gmail.com. Alghifarighaly@gmail.com

**Abstract**

The advancement of digital technology has significantly impacted defense communication systems, including those within the Indonesian Navy (TNI AL). Integrated communication systems enable rapid and efficient coordination of maritime operations, but at the same time, they introduce vulnerabilities to cyber threats. This article explores the urgency of enhancing cybersecurity within TNI AL's integrated communication systems, identifies various types of cyber threats, and outlines technical and organizational strategies that can be implemented to mitigate these risks. Using a literature review and comparative study approach, this paper provides recommendations to strengthen cyber defense systems, ensuring the continuity of maritime operations and maintaining information superiority in naval warfare.

**Keywords:** Cybersecurity; Integrated Communication; Indonesian Navy; Naval Operations; Data Encryption.

**Abstrak**

Kemajuan teknologi digital telah memberikan dampak besar terhadap sistem komunikasi pertahanan, termasuk di lingkungan TNI AL. Sistem komunikasi terpadu memungkinkan koordinasi operasi laut yang cepat dan efisien, namun pada saat yang sama membuka celah terhadap ancaman keamanan siber. Artikel ini membahas urgensi peningkatan keamanan siber dalam sistem komunikasi TNI AL, jenis-jenis ancaman yang dihadapi, serta strategi teknis dan organisasi yang dapat diterapkan untuk memitigasi risiko. Dengan pendekatan literatur dan studi komparatif, makalah ini memberikan rekomendasi penguatan sistem pertahanan siber untuk menjamin keberlanjutan operasi maritim dan menjaga superioritas informasi di medan laut.

**Kata kunci:** Keamanan Siber; Komunikasi Terpadu; TNI AL; Operasi Laut; Enkripsi Data.

## 1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi di era digital saat ini telah membawa perubahan mendasar dalam berbagai sektor, termasuk bidang pertahanan dan keamanan negara. TNI Angkatan Laut sebagai salah satu komponen utama pertahanan negara di matra laut dituntut untuk mampu beradaptasi dengan dinamika ancaman serta mengoptimalkan pemanfaatan teknologi dalam setiap aspek operasionalnya. Salah satu wujud konkret dari modernisasi tersebut adalah penerapan **sistem komunikasi terpadu**, yakni sistem komunikasi yang mengintegrasikan berbagai media dan platform—baik radio, satelit, data link, maupun jaringan komputer dalam satu kesatuan jaringan informasi yang mendukung komando, kendali, komunikasi, komputer, dan intelijen (C4I).

Sistem komunikasi terpadu memungkinkan pelaksanaan operasi maritim secara lebih cepat, akurat, dan efisien. Informasi taktis dan strategis dapat didistribusikan secara real-time dari pos

komando ke unsur-unsur laut maupun sebaliknya. Namun, kemajuan ini juga membawa tantangan baru, terutama terkait dengan **ancaman keamanan siber** yang semakin kompleks dan sulit diprediksi. Komunikasi militer yang dulunya bersifat tertutup dan lokal kini menjadi terbuka terhadap risiko intersepsi, sabotase digital, serangan malware, hingga manipulasi data melalui celah pada sistem atau kelalaian manusia (NIST, 2018; NATO, 2021). Ancaman-ancaman ini tidak hanya berpotensi mengganggu jalannya operasi, tetapi juga dapat melemahkan daya tangkal nasional jika tidak ditangani secara sistemik dan terintegrasi.

Urgensi penguatan keamanan siber dalam sistem komunikasi TNI AL diperkuat oleh fakta bahwa perang modern kini tidak lagi terbatas pada dimensi fisik, tetapi telah merambah ke domain informasi dan siber. Dominasi di medan pertempuran saat ini sangat ditentukan oleh kecepatan dan keandalan dalam mengelola informasi serta kemampuan mempertahankan integritas sistem komunikasi dari upaya penetrasi pihak musuh. Sebagaimana diungkapkan dalam laporan NATO (2021), komunikasi dan jaringan informasi militer menjadi target utama dalam konflik berbasis teknologi tinggi, karena gangguan sekecil apa pun pada sistem tersebut dapat berdampak luas terhadap komando dan pengambilan keputusan.

Oleh karena itu, diperlukan strategi pertahanan siber yang komprehensif, tidak hanya pada aspek teknis seperti enkripsi dan firewall, tetapi juga menyangkut pembentukan budaya keamanan informasi serta peningkatan kompetensi personel TNI AL dalam menghadapi dinamika perang siber. Beberapa negara telah menerapkan pendekatan ini secara terpadu melalui sistem zero trust, pelatihan personel secara berkala, serta penguatan kebijakan keamanan internal (Smith & Thomas, 2019).

Berdasarkan latar belakang tersebut, artikel ini bertujuan untuk mengkaji secara sistematis berbagai bentuk ancaman siber terhadap sistem komunikasi terpadu TNI AL, mengidentifikasi kelemahan-kelemahan utama yang dapat dimanfaatkan oleh pihak lawan, serta merumuskan strategi peningkatan keamanan siber yang relevan, aplikatif, dan berkelanjutan. Dengan pendekatan studi literatur dan komparatif terhadap praktik militer internasional, artikel ini diharapkan dapat memberikan kontribusi dalam penguatan sistem pertahanan komunikasi di lingkungan TNI AL sebagai bagian dari pembangunan kekuatan maritim nasional yang modern, tangguh, dan adaptif.

## 2. Metode

Penelitian ini menggunakan pendekatan deskriptif-kualitatif berbasis studi literatur. Sumber data diperoleh dari dokumen kebijakan pertahanan nasional, jurnal ilmiah, laporan teknis militer, serta standar internasional dari lembaga seperti NATO dan NIST. Target atau sasaran kajian dalam artikel ini adalah sistem komunikasi terpadu yang digunakan oleh TNI AL, khususnya yang terpasang di Kapal Perang Republik Indonesia (KRI) dan satuan komando pendukung lainnya. Analisis difokuskan pada identifikasi potensi ancaman siber, evaluasi kelemahan sistem, serta perumusan strategi penguatan keamanan siber yang aplikatif dan relevan dengan kebutuhan operasional TNI AL. Pemilihan pendekatan ini bertujuan untuk menghasilkan rekomendasi yang kontekstual dan dapat diimplementasikan secara bertahap sesuai kondisi infrastruktur komunikasi TNI AL saat ini.

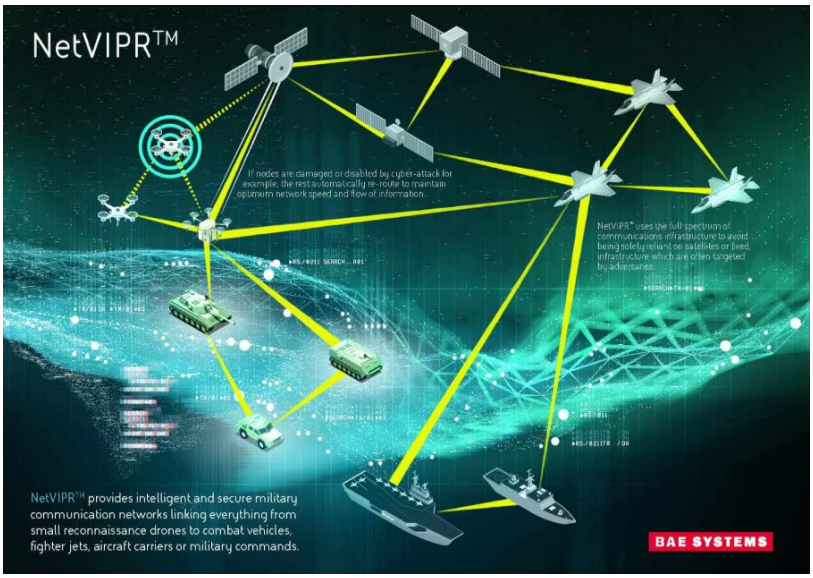
## 3. Hasil dan Pembahasan

Hasil analisis studi literatur menunjukkan bahwa sistem komunikasi terpadu TNI AL saat ini menghadapi tantangan serius dari aspek keamanan siber. Keberadaan jaringan data, radio, dan satelit yang saling terhubung memberikan efisiensi dalam koordinasi operasi laut, namun juga memperluas permukaan serangan siber. Data dari sumber Kementerian Pertahanan dan laporan

NATO menunjukkan bahwa sistem militer di banyak negara telah mengalami upaya intersepsi dan jamming dari pihak musuh.

**Tabel 1. Jenis Ancaman Siber terhadap Sistem Komunikasi Terpadu**

| No | Jenis Ancaman | Dampak terhadap Operasi Laut |
|---|---|---|
| 1 | Intersepsi Data | Kebocoran informasi misi dan lokasi unit operasional |
| 2 | Jamming Frekuensi | Terputusnya komunikasi antar-KRI dan komando pusat |
| 3 | Malware/Ransomware | Gangguan sistem kendali elektronik dan perangkat lunak |
| 4 | Spoofing Sinyal | Pemalsuan informasi posisi atau identitas KRI |
| 5 | Insider Threat | Kebocoran data oleh personel internal |




Gambar 1. Permukaan Serangan Siber dalam Sistem Komunikasi TNI AL

### 3.1. Strategi Mitigasi Ancaman Siber

Untuk menanggulangi ancaman-ancaman tersebut, diperlukan strategi pertahanan berlapis yang melibatkan teknologi dan manajemen personel.

#### 3.1.1. Pendekatan Teknis

Langkah teknis yang disarankan meliputi:

1) Implementasi enkripsi data tingkat militer, baik pada komunikasi radio maupun satelit.
2) Penggunaan sistem otentikasi multi-faktor bagi akses ke sistem komunikasi.
3) Pemanfaatan firewall militer dan intrusion detection system (IDS) untuk memantau lalu lintas jaringan secara real-time.
4) Penerapan arsitektur zero trust: setiap permintaan akses divalidasi terlepas dari lokasi jaringan.
5) Penguatan segmentasi jaringan, memisahkan jalur komunikasi sensitif dari jaringan terbuka.

### 3.1.2. Pendekatan Organisasi dan Personel

Di sisi organisasi:

1) Diperlukan standar operasional prosedur (SOP) pengamanan siber yang ketat di seluruh KRI dan pangkalan.

2) Personel elektronika perlu menjalani pelatihan keamanan siber secara berkala, termasuk simulasi serangan.

3) Dibentuknya unit siber taktis yang bertugas mendeteksi dan merespon insiden siber dalam waktu nyata.

4) Audit keamanan berkala terhadap sistem komunikasi elektronik.

## 4. Simpulan

Peningkatan keamanan siber pada sistem komunikasi terpadu TNI Angkatan Laut merupakan suatu kebutuhan strategis yang tidak dapat ditunda, mengingat transformasi digital yang terus berlangsung dalam lingkungan pertahanan nasional dan global. Sistem komunikasi terpadu, yang mencakup jaringan radio, satelit, dan data link, telah menjadi tulang punggung dalam mendukung efektivitas komando dan pengendalian operasi laut modern. Namun, di sisi lain, kompleksitas sistem dan keterhubungan yang tinggi juga memperbesar potensi celah keamanan yang dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab. Ancaman seperti intersepsi data, jamming frekuensi, spoofing sinyal, hingga serangan malware terhadap infrastruktur komunikasi dapat mengganggu jalannya operasi, membahayakan keselamatan personel, serta mengancam kerahasiaan informasi strategis TNI AL.

Melalui kajian literatur dan studi komparatif, telah diidentifikasi bahwa tantangan utama dalam pengamanan komunikasi militer adalah lemahnya standar keamanan siber yang konsisten, keterbatasan sistem deteksi dini terhadap serangan digital, serta kurangnya pelatihan personel dalam menghadapi ancaman berbasis teknologi informasi. Oleh karena itu, solusi yang direkomendasikan meliputi penerapan sistem enkripsi end-to-end, pembangunan arsitektur jaringan berbasis prinsip zero trust, penguatan segmentasi komunikasi internal, serta peningkatan kapasitas SDM melalui pelatihan dan simulasi keamanan siber secara berkala. Tidak kalah penting adalah pengadaan perangkat komunikasi militer yang telah tersertifikasi dan teruji keamanannya sesuai standar pertahanan nasional maupun internasional.

Secara keseluruhan, keberhasilan implementasi sistem komunikasi yang aman dan andal di lingkungan TNI AL akan sangat menentukan kesiapsiagaan tempur, efektivitas operasi laut, serta dominasi informasi di medan perang maritim masa depan. Sinergi antara penguatan teknologi, kebijakan organisasi, dan kompetensi personel menjadi kunci utama dalam membangun sistem komunikasi pertahanan yang tangguh dan adaptif di era digital yang penuh tantangan ini.

## 5. Daftar Rujukan

Kementerian Pertahanan Republik Indonesia. (2022). Strategi Keamanan Siber Nasional. Jakarta, Indonesia: Pusdatin Kemhan.

NATO. (2021). Cybersecurity in military operations. Brussels, Belgium: NATO Review Publications.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). Gaithersburg, MD: U.S. Department of Commerce.

Sutaryo, A., & Prasetyo, H. (2020). Sistem komunikasi militer TNI dan tantangan era digital. Jurnal Pertahanan, 10(1), 45–58.

Smith, R., & Thomas, L. (2019). Military communications: Security and resilience. Berlin, Germany: Springer..

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: U.S. Department of Commerce.

Smith, R., & Thomas, L. (2019). Military Communications: Security and Resilience. Berlin, Germany: Springer.