Jurnal Syntax Imperatif: Jurnal Ilmu Sosial dan Pendidikan
Volume 6, No 5, November 2025, pp. 1387-1395
P-ISSN: 2721-2491 E-ISSN: 2721-2491
DOI: http://doi.org/10.54543/syntaximperatif.v6i5.846
Published By: CV. Rifainstitut

Analisis Peran C5ISR Sistem Komando dan Pengendalian TNI Angkatan Laut dalam Menghadapi Ancaman Siber di ALKI I

Eska Wiratama[1], Buddy Suseto[2], Ditto Regina Saputra[3]
[1,2,3] Sekolah Staf dan Komando TNI AL, Indonesia

ARTICLE INFO

Article history:
Received October 06, 2025
Revised December 20, 2025
Accepted December 31, 2025
Available online December 31, 2025

Kata Kunci :
C5ISR, ALKI I, TNI Angkatan Laut, Ancaman Siber, Komando dan Kendali, Pertahanan Maritim

Keywords:
C5ISR, ALKI I, Indonesian Navy, Cyber Threats, Command and Control, Maritime Defense

ABSTRAK

Sebagai negara kepulauan, Indonesia menghadapi tantangan serius dalam menjaga kedaulatan maritim, khususnya di Alur Laut Kepulauan Indonesia I (ALKI I) yang memiliki nilai strategis tinggi. Ancaman siber terhadap sistem pertahanan maritim semakin nyata, ditandai dengan insiden seperti peretasan AIS, serangan DDoS, dan spionase data. Penelitian ini bertujuan untuk menganalisis peran sistem Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance (C5ISR) TNI Angkatan Laut dalam menghadapi ancaman siber di ALKI I. Fokus utama diarahkan pada kesiapan sistem komando dan kendali di Koarmada I serta efektivitas pemanfaatan C5ISR dalam mendeteksi, mencegah, dan merespons serangan siber. Pendekatan yang digunakan adalah kualitatif, melalui wawancara mendalam, observasi, dan analisis dokumen, dengan pengolahan data secara sistematis menggunakan perangkat lunak NVivo. Hasil yang diharapkan mencakup pemetaan kondisi terkini sistem C5ISR, identifikasi kesenjangan integrasi teknologi informasi, serta penyusunan rekomendasi kebijakan dan strategi peningkatan kapasitas pertahanan siber TNI AL. Kebaruan penelitian ini terletak pada integrasi konsep pertahanan siber dalam kerangka C5ISR pada konteks maritim, serta penerapan pendekatan kualitatif dalam kajian pertahanan. Temuan penelitian diharapkan dapat berkontribusi dalam memperkuat pertahanan maritim Indonesia di era digital, sekaligus meningkatkan situational awareness dan interoperabilitas sistem di kawasan strategis yang rentan seperti ALKI I.

ABSTRACT

As an archipelagic nation, Indonesia faces serious challenges in safeguarding maritime sovereignty, particularly in the strategically vital Indonesian Archipelagic Sea Lane I (ALKI I). Cyber threats to maritime defense systems are becoming increasingly evident, marked by incidents such as AIS hacking, DDoS attacks, and data espionage. This study aims to analyze the role of the Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance (C5ISR) system of the Indonesian Navy in countering cyber threats in ALKI I. The primary focus is directed toward the readiness of the command and control system at Fleet Command I (Koarmada I) and the effectiveness of utilizing C5ISR in detecting, preventing, and responding to cyberattacks. A qualitative approach is employed, using in-depth interviews, observations, and document analysis, with data processed systematically using NVivo software. The expected outcomes include mapping the current state of the C5ISR system, identifying integration gaps in information technology, and providing policy recommendations and capacity-building strategies for the Navy's cyber defense. The novelty of this study lies in the integration of cyber defense concepts within the C5ISR framework in a maritime context, and the application of a qualitative approach in defense studies. The findings are expected to contribute to strengthening Indonesia's maritime defense in the digital era, while enhancing situational awareness and system interoperability in strategically vulnerable areas such as ALKI I.

1. PENDAHULUAN

Indonesia memiliki wilayah laut yang luas dengan jalur pelayaran strategis, salah satunya adalah ALKI I. Jalur ini menghubungkan Laut Cina Selatan ke Samudra Hindia melalui Selat Sunda, dan menjadi rute penting bagi kapal dagang dan militer (Hermawan & Sutanto, 2022). ALKI merupakan koridor bagi pelayaran internasional yang menghubungkan Samudra Pasifik dan Samudra Hindia melintasi perairan Indonesia. Terdapat tiga jalur ALKI utama (ALKI I, II,

*Corresponding author
E-mail addresses: Eskawiratama54@gmail.com (Eska Wiratama)

dan III); ALKI I meliputi rute dari Laut Cina Selatan/Natuna melalui Selat Karimata, Laut Jawa, hingga Selat Sunda menuju Samudra Hindia. Tingginya trafik kapal dagang maupun militer di ALKI I menjadikan kawasan ini sangat strategis sekaligus rawan ancaman. Karena kepadatan lalu lintasnya, ALKI I sangat strategis namun juga rawan terhadap berbagai ancaman, termasuk serangan siber.

Untuk menjaga keamanan, TNI AL telah memasang sistem pengawasan seperti *Integrated Maritime Surveillance System* (IMSS) di sejumlah titik penting. Namun, tantangan tidak hanya datang dari pelanggaran fisik seperti penyelundupan, tetapi juga dari serangan digital. Serangan siber dapat mengganggu sistem navigasi dan komunikasi kapal, bahkan menonaktifkan sistem komando. Ancaman siber kini menjadi bagian dari strategi militer global. Beberapa negara telah mengembangkan kemampuan *cyber warfare* yang bisa digunakan secara mandiri atau bersamaan dengan konflik fisik. Contoh kasus seperti serangan siber Hamas terhadap infrastruktur Israel yang dibalas dengan serangan langsung menunjukkan betapa seriusnya ancaman ini.

Pertahanan maritim tidak lagi cukup berfokus pada ancaman fisik semata, namun juga perlu mengantisipasi serangan di dunia maya. TNI Angkatan Laut sebagai garda terdepan pertahanan laut Nusantara, dituntut untuk memanfaatkan kemajuan teknologi informasi dan komunikasi guna mencapai keunggulan informasi dalam setiap operasi. Konsep *Command, Control, Communications, Computers, Combat System, Intelligence, Surveillance and Reconnaissance* (C5ISR) (Khotimah, N. N., & Hendra, A., 2023) menjadi kerangka penting dalam integrasi teknologi tersebut. Dengan sistem C5ISR yang handal.

Tabel 1. Matriks Pelanggaran di ALKI I

No.	Waktu	Jenis Serangan	Pelaku Terindikasi	Target/Sistem yg diserang	Dampak	Respon Indonesia	Sumber
1.	Feb 2024	GPS Spoofing	Kelompok APT31 – Tiongkok	MT. OCEAN PRIDE (tanker)	Gangguan Navigasi Selat Sunda	Investigasi oleh Pushidrosal & Bakamla	Laporan BSSN
2.	Apr 2024	Peretasan AIS	Kapal Ikan Vietnam	Manipulasi Identitas Kapal	Memfasilitasi illegal fishing	Penenggelaman kpl oleh KKP	KKP Press Release
3.	Jun 2024	Ransomware Pelabuhan	Grup Dark Seas	Sistem IT pelabuhan benoa	Gangguan Operasional selama 72 Jam	Pemulihan Data oleh BSSN	Kompas Cyber Attack
4.	Sep 2024	Spionase Data Hidrografi	APT 41 (tiongkok)	Database Pushidrosal	Akebocoran Data survei Dasar Laut	Pembaruan Sistem Keamanan	Jnes Defence
5.	Jan 2025	DDoS Bakamla	Hactivist Anonymous sea	Sistem Komunikasi Bakamla	Gangguan Koordinasi Bakamla	Mitigasi BSSN dan TNI AL	Tempo Cyber

Sumber: BSSN, TNI AL, Laporan Media Siber & Open Source, 2025

Data tersebut menunjukkan bahwa serangan siber di ALKI I bersifat terorganisir dan berdampak langsung terhadap navigasi, sistem data, dan kesiapan operasional. Oleh karena itu, informasi yang cepat dan akurat melalui sistem C5ISR menjadi krusial. Sistem ini mampu memberikan keunggulan dalam hal situational awareness dan koordinasi respons.

ALKI I yang melintasi Selat Sunda menjadi salah satu titik rawan karena sifatnya sebagai *choke point*. Potensi serangan siber di kawasan ini meliputi peretasan radar pantai, manipulasi AIS, *jamming* komunikasi kapal-pusat, hingga *malware* pada sistem komando (Sarjito & ASEAN Eng., 2025). Jika sistem C5ISR berhasil ditembus, maka deteksi dan respon terhadap ancaman fisik pun akan terganggu. Penguatan sistem C5ISR terhadap ancaman siber akan memastikan *situational awareness* tetap terjaga dan kendali operasi tidak terganggu. Oleh sebab itu, analisis mengenai peran sistem C5ISR TNI Angkatan Laut dalam menghadapi ancaman siber di ALKI I menjadi sangat penting.

2. KAJIAN LITERATUR

Untuk melakukan analisis dan memahami lebih dalam permasalahan yang terjadi, peneliti menggunakan beberapa teori sebagai panduan dalam melakukan analisis terhadap masalah yang dihadapi. Tinjuan teori yang ada dalam penelitian ini menjelaskan tentang teori-teori dan konsep yang berkaitan dengan permasalahan penelitian serta penelitian terdahulu sebagai pembanding dan menjaga orisinalitas dalam penyusunan penelitian sesuai dengan variabel dalam penelitian ini yaitu penerapan-penerapan sistem C5ISR dalam menghadapi ancaman Asimetris di ALKI I.

Konsep C5ISR

C5ISR merupakan sistem terintegrasi untuk mendukung dominasi informasi dalam operasi militer. Sistem ini terdiri atas *Command and Control* (proses pengambilan keputusan), *Communications dan Computers* (jaringan komunikasi dan pemrosesan data), serta *Intelligence, Surveillance, dan Reconnaissance* (pengumpulan dan pemantauan informasi). Fungsinya meliputi deteksi ancaman melalui sensor, pengolahan data oleh intelijen, hingga pemberian perintah taktis kepada unit tempur. C5ISR mempercepat siklus *Observe Orient Decide Act* (OODA), sehingga meningkatkan kecepatan dan ketepatan keputusan operasi (Byus, 2018).

Konsep Strategi Militer (*Ends-Ways-Means*)

Strategi mili*ter adalah seni dan ilmu mengatur cara (ways), sarana (means), dan tujuan (*ends) untuk mencapai kepentingan pertahanan. Menurut Liddell Hart (2012) dan Good Paster, unsur strategi terdiri dari: apa yang ingin dicapai (ends), bagaimana mencapainya (ways) dan dengan apa tujuan itu diwujudkan (means). Ketiga elemen ini harus disusun secara seimbang dan dapat beradaptasi terhadap situasi yang berubah dalam lingkungan strategis.

Ancaman Siber dalam Pertahanan Maritim

Ancaman siber merupakan tantangan baru dalam pertahanan maritim yang menyasar infrastruktur informasi seperti sistem navigasi, radar, hingga satelit komunikasi militer. Jenis serangan mencakup malware, phishing, DDoS, dan peretasan sistem pelabuhan atau komando. Menurut Salim (2024), diperlukan komponen seperti enkripsi, firewall, dan sistem deteksi intrusi untuk melindungi jaringan. Pendekatan sistem C5ISR yang mengintegrasikan deteksi dini, komando, dan pengawasan digital sangat penting dalam merespons ancaman ini, terutama di wilayah strategis seperti ALKI I.

Evolusi Sistem Komando dan Kendali

Sistem komando militer telah berevolusi mulai dari C2 (komando dan kendali dasar), C3 (penambahan komunikasi), C4 (penambahan komputerisasi), hingga C4ISR (penguatan intelijen dan pengawasan). Tahap berikutnya, C5ISR menambahkan integrasi sistem tempur. Kini berkembang menjadi C6ISR yang menyatukan sistem siber, senjata, sensor, dan informasi

dalam satu arsitektur digital tempur. Transformasi ini menjawab kebutuhan militer modern untuk pengendalian yang cepat, presisi, dan berbasis jaringan.

Sejumlah studi sebelumnya menyoroti pentingnya integrasi sistem pengawasan dan teknologi informasi dalam pertahanan maritim. Lathif et al. (2022) menilai IMSS di ALKI I efektif meningkatkan pengawasan, namun menghadapi kendala koordinasi internal. Tesis Novie Adolof (2022) menunjukkan bahwa penguatan C4ISR di kapal LPD berdampak signifikan terhadap efektivitas operasi, terutama melalui integrasi komunikasi satelit dan sistem data taktis.

Allim et al. (2019) mengusulkan sistem pengawasan bawah laut berbasis akustik untuk deteksi kapal selam, menekankan pentingnya integrasi sensor dalam sistem C4ISR nasional. Juanita et al. (2021) menyoroti lemahnya interoperabilitas informasi antara TNI AL dan Bakamla. Sementara itu, Hadiwijaya (2022) menekankan pentingnya sistem komando jarak jauh berbasis satelit untuk patroli wilayah strategis. Praja (2021) menyoroti ancaman siber sebagai bagian dari strategi militer global dan pentingnya digitalisasi sistem pertahanan.

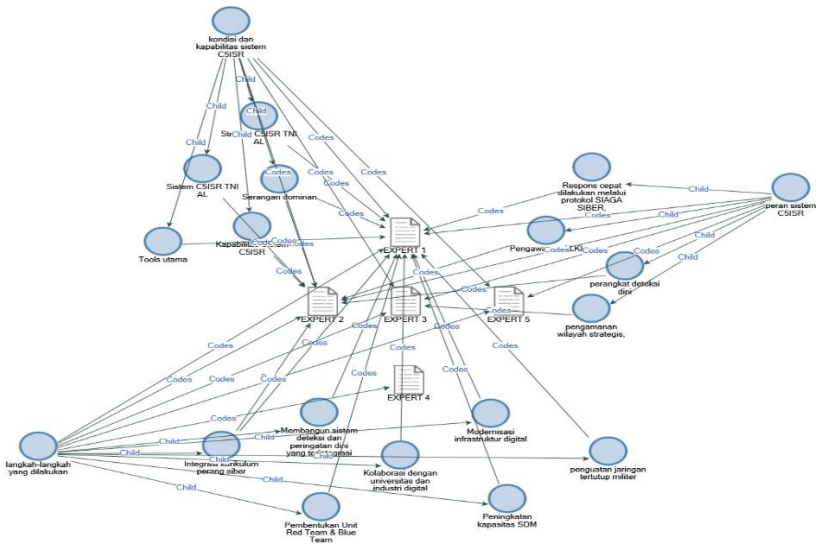
Meskipun berbagai studi membahas C4ISR dan pengawasan maritim, belum ada yang secara khusus mengkaji peran sistem C5ISR TNI AL dalam menghadapi ancaman siber di ALKI I, menjadikan topik ini relevan dan penting untuk diteliti lebih lanjut.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan strategi studi kasus, yang difokuskan pada Koarmada I sebagai pusat operasional TNI AL di wilayah ALKI I. Data primer dikumpulkan melalui wawancara semi-terstruktur dengan pejabat kunci seperti Kepala Puskodal, Perwira Komunikasi, dan staf siber, untuk menggali pengalaman serta strategi menghadapi ancaman siber. Data tambahan diperoleh dari dokumentasi operasional dan observasi non-partisipatif di fasilitas komando guna memvalidasi prosedur pemanfaatan sistem C5ISR. Seluruh data dianalisis menggunakan NVivo melalui proses coding tematik dan pengelompokan pola, dengan validasi dilakukan melalui triangulasi sumber dan teknik. Peneliti juga terlibat secara terbatas untuk memahami dinamika pengambilan keputusan, sementara audit trail digunakan untuk memastikan transparansi dan keandalan analisis.

Pengolahan Data (NVivo)

Setelah data terkumpul, langkah berikutnya adalah pengolahan data kualitatif. Tahapan pengolahan dibantu NVivo secara garis besar sebagai berikut:

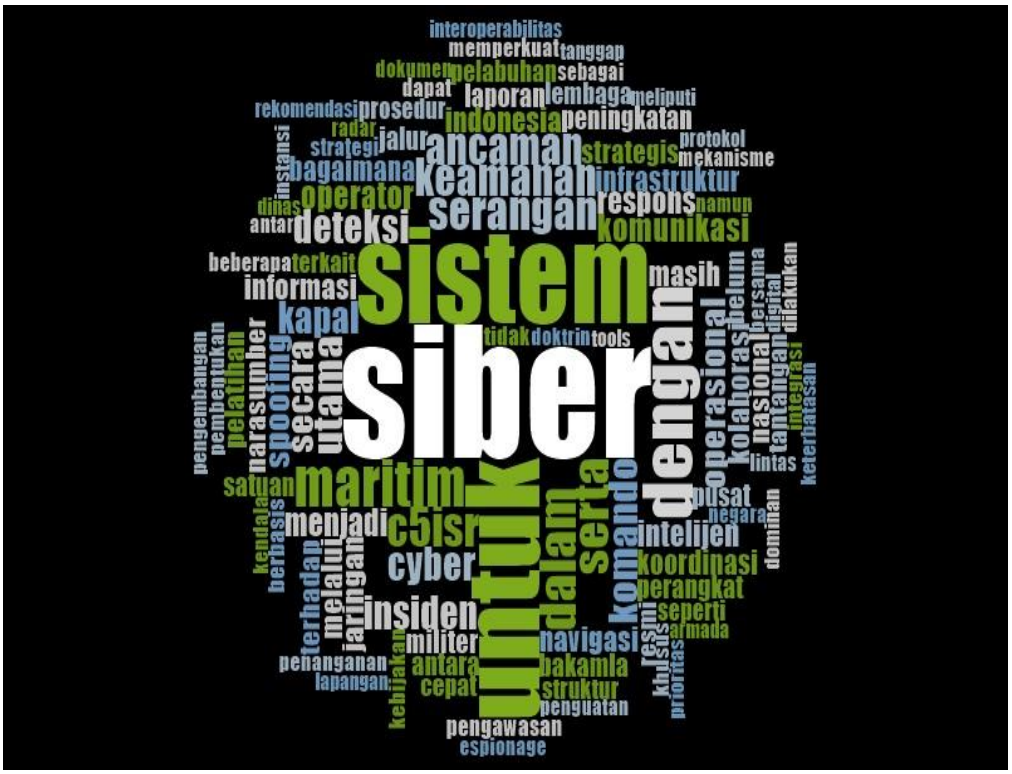


Gambar 1. Coding Nvivo
Sumber: Hasil Olahan Peneliti, 2025

Visualisasi hasil pengolahan data menggunakan perangkat lunak NVivo menunjukkan struktur tematik yang merepresentasikan secara kuat pandangan para narasumber mengenai peran, kondisi, dan strategi pemanfaatan sistem C5ISR oleh TNI AL, khususnya Koarmada I, dalam menghadapi ancaman siber di wilayah ALKI I. Peran sistem C5ISR tergambarkan melalui keterkaitannya dengan node-node seperti deteksi dini, pengawasan, pengamanan wilayah strategis, dan respon cepat, yang menempatkan C5ISR sebagai tulang punggung sistem komando dan pengendalian berbasis informasi real-time. Dalam konteks kapabilitas, hasil pengolahan data menunjukkan bahwa sistem ini masih menghadapi keterbatasan integrasi antar satuan, keterbatasan dalam otomatisasi, serta perlunya pembaruan perangkat deteksi dan komputasi untuk menjangkau seluruh wilayah rawan di ALKI I. Selain itu, dimensi strategi menunjukkan bahwa TNI AL telah memulai berbagai langkah seperti pembentukan *Unit Red Team & Blue Team*, kolaborasi dengan sektor sipil, serta modernisasi infrastruktur dan peningkatan SDM. Meskipun demikian, mayoritas inisiatif tersebut masih berada dalam tahap pengembangan awal, sehingga diperlukan penguatan implementasi yang lebih menyeluruh untuk memastikan sistem C5ISR benar-benar berfungsi secara adaptif dan responsif terhadap spektrum ancaman siber yang semakin kompleks.

Teknik Analisis Data

Analisis data merupakan suatu fase penelitian kualitatif yang sangat penting karena melalui analisis data tersebut peneliti dapat memperoleh wujud dari penelitian yang telah dilakukan. Analisis adalah suatu upaya mengurai menjadi bagian-bagian (*decomposition*), sehingga susunan/tata bentuk sesuatu yang dideskripsikan terlihat jelas dipahami atau permalahannya dapat lebih jelas dipahami.



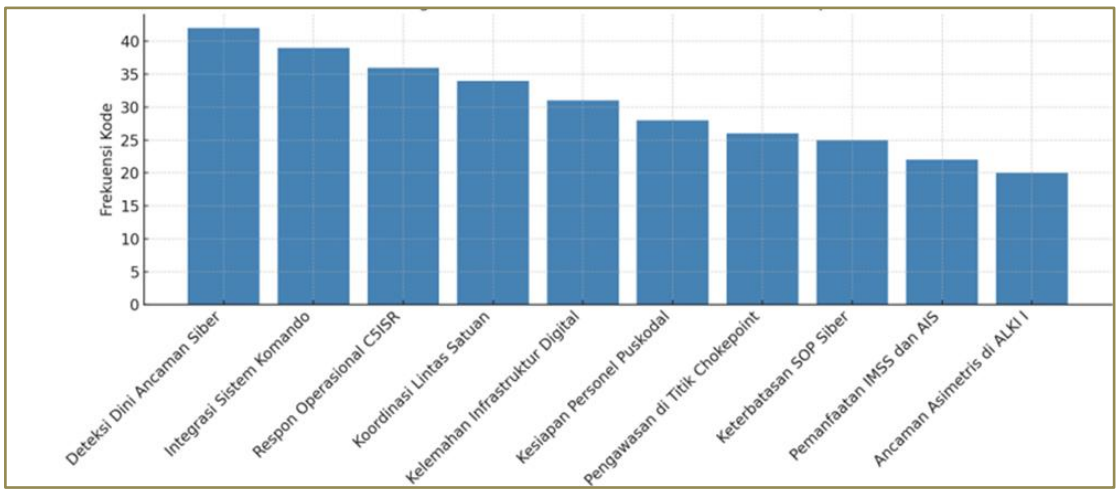
Gambar 2 *Word Cloud Nvivo*

Sumber: Hasil Olahan Peneliti,2025

Analisis data *word cloud* dari wawancara para informan menampilkan kata-kata kunci seperti "siber", "sistem", "maritim", "keamanan", "deteksi" dan "komando" sebagai fokus tematik utama, yang mencerminkan persepsi kolektif terhadap pentingnya sistem C5ISR dalam pertahanan laut Indonesia. Dominasi kata "komando", "deteksi", dan "pengawasan" menunjukkan bahwa sistem ini diposisikan sebagai pilar utama komando dan pengendalian, yang mendukung kesadaran situasional, peringatan dini, serta kemampuan pengambilan keputusan cepat berbasis informasi *real-time*. Sementara itu, frekuensi tinggi dari kata seperti "struktur", "kapasitas", "terbatas" dan "koordinasi" menggambarkan bahwa sistem C5ISR saat ini masih menghadapi berbagai keterbatasan, baik dalam hal infrastruktur, konektivitas antar satuan, maupun kesiapan personel dalam menangani ancaman digital. Kemunculan kata "tidak doktrin" dan "belum SOP" mengindikasikan bahwa kebijakan dan standar operasional dalam aspek siber masih perlu diperkuat. Di sisi lain, keberadaan kata "modernisasi", "penguatan", "pengembangan", dan "red team" mencerminkan adanya kesadaran institusional untuk melangkah menuju penguatan kapasitas, melalui integrasi dengan industri digital, peningkatan sistem tertutup militer, serta pembentukan unit respons siber yang adaptif. Secara keseluruhan, visualisasi ini menegaskan bahwa sistem C5ISR telah menjadi bagian strategis dalam menghadapi tantangan siber di wilayah ALKI I, namun pengembangannya masih memerlukan konsistensi, modernisasi menyeluruh, dan kesiapan sumber daya manusia yang andal untuk menjamin ketahanan dan efektivitas sistem dalam jangka panjang.

4. HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa sistem C5ISR TNI AL di wilayah ALKI I telah diterapkan melalui integrasi sistem pengawasan maritim berbasis radar pantai, sensor kapal, serta pusat komando (Puskodal). Namun, tantangan signifikan masih dihadapi dalam hal interoperabilitas antarsatuan, kesiapan personel, serta ketahanan sistem terhadap serangan siber.



Gambar 3 Visualisasi Hasil *Nvivo*

Sumber: Hasil Olahan Peneliti,2025

Hasil analisis menggunakan perangkat lunak NVivo mengungkap sejumlah tema dominan dari wawancara dengan para informan di lingkungan Koarmada I. Tiga tema utama yang muncul adalah: Deteksi Dini Ancaman Siber (42 frekuensi), Integrasi Sistem Komando (39 frekuensi) dan Respon Operasional C5ISR (36 frekuensi). Temuan ini menunjukkan bahwa perhatian terbesar tertuju pada kesiapan sistem dalam mengidentifikasi gangguan digital sejak dini, kendala koordinasi lintas satuan, serta kebutuhan akan respons cepat dan terstandarisasi

terhadap serangan siber. Visualisasi data word cloud juga memperkuat dominasi kata kunci seperti "komando", "deteksi", "koordinasi", "respon", dan "siber".

Analisis tersebut diperkuat dengan temuan dari studi Rakhmadi (Rakhmadi et al., 2025) mengenai *coastal defense*, yang menekankan pentingnya integrasi antara intelijen, komando dan pengawasan. Model *Interpretive Structural Modeling* (ISM) yang digunakan dalam penelitian tersebut mengidentifikasi ketiga faktor tersebut sebagai elemen pengungkit yang sangat berpengaruh terhadap ketahanan sistem pertahanan maritim. Dengan pendekatan serupa, sistem C5ISR di TNI AL dapat diarahkan untuk memperkuat integrasi peran intelijen siber serta koordinasi antar unsur komando dan operasional.

Kendala implementasi sistem C5ISR di ALKI I meliputi terbatasnya interoperabilitas antar sistem, kurangnya kesiapan personel dalam menangani insiden siber dan belum adanya SOP penanganan siber yang menyeluruh. Hal ini menunjukkan bahwa sistem C5ISR masih perlu ditingkatkan agar dapat berfungsi optimal sebagai tulang punggung pertahanan informasi di wilayah maritim Indonesia.

Sistem C5ISR memiliki potensi besar untuk mendukung pertahanan digital TNI AL, namun saat ini belum sepenuhnya terintegrasi dan responsif terhadap spektrum ancaman siber. Temuan menunjukkan bahwa Puskodal dan unit terkait masih bekerja dalam silo informasi, yang menghambat efektivitas koordinasi dan kecepatan pengambilan keputusan.Jika dibandingkan dengan model coastal defense berbasis ISM, sistem C5ISR TNI AL cenderung didominasi oleh aspek teknis, sementara faktor-faktor kunci seperti intelijen, pengawasan, dan komando belum sepenuhnya diintegrasikan secara sistemik. Untuk itu, penting bagi TNI AL mengembangkan struktur C5ISR yang mampu menjalin keterhubungan antar elemen dan memperkuat fungsi komando digital.

Strategi peningkatan sistem disarankan dalam beberapa bentuk: pembentukan detasemen siber khusus, pelatihan rutin berbasis simulasi, pembaruan SOP, serta integrasi sistem dengan institusi eksternal seperti BSSN dan Bakamla. Dengan cara ini, sistem C5ISR dapat lebih adaptif dan mampu menjawab kebutuhan pertahanan modern yang mencakup dimensi fisik dan digital. C5ISR TNI AL berperan penting dalam mempertahankan ALKI I dari ancaman siber, namun realisasinya membutuhkan langkah-langkah penguatan struktural, teknologis, dan sumber daya manusia secara berkelanjutan untuk mencapai sistem pertahanan maritim yang unggul dan adaptif terhadap dinamika era digital.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa sistem C5ISR TNI AL memiliki peran yang sangat krusial dalam menghadapi ancaman siber di kawasan strategis ALKI I. Sistem ini tidak hanya berfungsi sebagai pendukung pengawasan dan komunikasi, tetapi juga menjadi instrumen utama dalam deteksi dini ancaman digital serta dalam mendukung pengambilan keputusan berbasis informasi real-time. Namun demikian, hasil wawancara dan analisis menggunakan NVivo mengungkap bahwa implementasi C5ISR di lingkungan Koarmada I masih menghadapi sejumlah tantangan mendasar, seperti terbatasnya interoperabilitas sistem antar satuan, kurang optimalnya pelatihan personel dalam penanganan ancaman siber, serta belum tersedianya dokumen SOP yang standar dan komprehensif. Kondisi ini menunjukkan bahwa kesiapan sistem C5ISR dalam menghadapi spektrum ancaman modern di domain maritim digital masih perlu ditingkatkan. Temuan tersebut diperkuat oleh studi komparatif terhadap model coastal defense berbasis ISM yang menekankan pentingnya integrasi fungsi intelijen, komando, dan pengawasan sebagai fondasi utama sistem pertahanan yang adaptif dan responsif.

Berdasarkan temuan tersebut, penguatan sistem C5ISR TNI AL di wilayah ALKI I perlu diarahkan pada langkah-langkah strategis yang terintegrasi dan berkelanjutan. Upaya ini dapat dilakukan melalui pembentukan unit siber khusus di bawah Komando Armada yang berfungsi sebagai detasemen tanggap cepat terhadap serangan siber, sehingga respons terhadap insiden

digital dapat dilakukan secara lebih terkoordinasi dan efektif. Selain itu, pelaksanaan pelatihan siber secara berkala dengan skenario ancaman berbasis simulasi digital menjadi penting untuk meningkatkan kapasitas dan kesiapsiagaan personel dalam menghadapi dinamika ancaman yang terus berkembang. Penguatan tersebut juga harus didukung dengan pembangunan integrasi sistem C5ISR TNI AL dengan instansi keamanan nasional lainnya, seperti BSSN dan Bakamla, guna mewujudkan sistem pertahanan maritim digital yang holistik, adaptif, dan mampu menjawab tantangan keamanan di era transformasi digital.

6. UCAPAN TERIMAKASIH

Peneliti menyampaikan terima kasih kepada Komando Armada I, para informan di lingkungan Puskodal TNI AL dan dosen pembimbing di SESKOAL atas bimbingan dan fasilitasi yang diberikan selama proses penelitian ini.

7. REFERENSI

Achjar, K. A. H., Rusliyadi, M., Zaenurrosyid, A., Rumata, N. A., Nirwana, I., & Abadi, A. (2023). Metode penelitian kualitatif: Panduan praktis untuk analisis data kualitatif dan studi kasus. PT. Sonpedia Publishing Indonesia.

ALKI. (n.d.). Saintek: Jurnal Sains Teknologi Dan Profesi Akademi Angkatan Laut, 15(2), 1417–1445.

Arianto, B., & Rani, R. (2024). Penyusunan state of the art penelitian.

Aryani, C. (2021). Mendorong lahirnya RUU keamanan laut dalam penguatan sistem keamanan laut nasional. Jurnal Pembangunan Hukum Indonesia, 3(2), 155–173.

Berkebile, R. E. (2018). Military strategy revisited: A critique of the Lykke formulation. Military Review, 7(May), 1–8.

Budiman, A., Ardipandanto, A., Fitri, A., & Dewanti, S. C. (2021). Pembangunan kekuatan minimum komponen utama pertahanan negara di era new normal. Publica Indonesia Utama.

Byus, K. (2018). Observe, orient, decide, act: A subjectivist model of entrepreneurial decision making. Journal of Managerial Issues, 349–362.

Carey, S. S. (2019). Kaidah-kaidah metode ilmiah: Panduan untuk penelitian dan critical thinking. Nusamedia.

Chadhafi, M. I. (2020). Risk register dalam aturan pelibatan: Rules of engagement. Media Nusa Creative (MNC Publishing).

Gultom, B. D., Hartono, D., & Simatupang, H. (2022). Pemberdayaan tata ruang laut di Koarmada I guna mendukung pembangunan postur TNI dalam rangka pertahanan negara. Jurnal Hidrografi Indonesia, 4(2), 111–120.

Hedhianto, A. T. (2024). Diplomasi pertahanan Indonesia terhadap New Zealand untuk mengatasi isu internasionalisasi Papua di dunia. Diplomacy and Global Security Journal: Jurnal Mahasiswa Magister Hubungan Internasional, 1(1).

Hermawan, T., & Sutanto, R. (2022). Strategi pertahanan laut Indonesia dalam analisa ancaman dan kekuatan laut. Jurnal Education and Development, 10(2), 363–371.

Kaunang, R. B. (2022). Penegakan hukum di wilayah zona ekonomi eksklusif Indonesia (Perairan Natuna Utara) sebagai kawasan klaim Laut China Selatan. Lex Administratum, 10(1).

Khotimah, N. N., & Hendra, A. (2023). Pengembangan sistem komunikasi dan radar serta instalasi senjata guna mendukung sistem pertahanan dan keamanan rakyat semesta (Sishankamrata). Jurnal Pengabdian Mandiri, 2(1), 405–414.

Legard, R., Keegan, J., & Ward, K. (2003). In-depth interviews. In J. Ritchie & J. Lewis (Eds.), Qualitative research practice: A guide for social science students and researchers (pp. 138–169). SAGE Publications.

Pranoto, H., & Octavian, A. (2015). Security strategy at Indonesia Archipelagic Sea Lane. Jurnal Pertahanan, 1(2), 93–108.

Purnomo, A. (2023). Penguatan sistem komando C5ISR dalam menghadapi ancaman siber di kawasan maritim Indonesia. Jurnal Strategi Pertahanan Maritim, 8(2), 112–129.

Qureshi, W. A. (2020). The rise of hybrid warfare. Notre Dame Journal of International & Comparative Law, 10, 173.

Rakhmadi, A. T. I., Khusaini, M., Puspitawati, D., Aminuddin, M. F., & Susilo, A. K. (2025). Exploring Key Factors of Coastal Defense System from Military Perspective in Surabaya Region using Delphi and Interpretive Structural Modeling. Journal of Maritime Research, 22(1), 35-49.

Salim. (2024). Basic knowledge of cyber security. Madani Berkah Abadi.

Sarjito, I. A., & Eng, A. S. E. A. N. (2025). Prinsip Sun Tzu dalam doktrin Angkatan Laut. Indonesia Emas Group.

Setyanto, L. (2024). Analisis pembinaan teritorial dalam peningkatan pemberdayaan sumber daya nasional. Jurnal Ekonomi Manajemen Sistem Informasi (JEMSI), 6(1).

Sianturi, D., Munir, M., & Sunny, A. G. (2023). Tantangan penggunaan artificial intelligence dalam hybrid warfare. Innovative: Journal of Social Science Research, 3(5), 9984–9996.

Sujarweni, V. W. (2014). Metodologi penelitian. Pustaka Baru Press.

Ţigănuş, D., & Alexandrescu, M. C. (2018). Considerations regarding the implementation of the architectural model for the development of command, control, communications, computers, intelligence. Romanian Military Thinking.

Simorangkir, V. O., Muchlis, N., Salamah, U., & Trijurini, A. (2022). Konsepsi penggunaan AUV sebagai underwater surveillance guna meningkatkan keamanan bawah air.

Wagenhals, L. W., Shin, I., Kim, D., & Levis, A. H. (2000). C4ISR architectures: II. A structured analysis approach for architecture design. Systems Engineering, 3(4), 248–287.

Wahyono, B. S. (2024). Pengembangan teknologi pertahanan berbasis C5ISR untuk kedaulatan wilayah laut NKRI. Jurnal Keamanan Nasional, 5(1), 45–62.