JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v6i2

Analisis Ancaman Hibrida terhadap Keamanan Maritim Indonesia dan Implikasi pada Postur TNI Angkatan Laut

Aldwin Hafidz Harsandy[1]
[1]Sekolah Staf dan Komando TNI Angkatan Laut (Seskoal), Indonesia,
aldwinhafidzharsandy@yahoo.com

Corresponding Author: aldwinhafidzharsandy@yahoo.com

Abstract: *Global and regional strategic environmental changes have given rise to hybrid threats that combine military and non-military elements. As an archipelagic nation with a vital geostrategic position, Indonesia faces high vulnerability to such threats, particularly in the maritime sector. This study aims to analyze the characteristics of hybrid threats affecting Indonesia's maritime security and assess their impact on the posture of the Indonesian Navy. Using a descriptive qualitative approach through content analysis of strategic defense documents, Global Fire Power data, and academic literature, the study identifies five major forms of hybrid threats: digital disinformation, cyberattacks, transnational crimes, economic infiltration, and proxy actions in maritime border areas. The findings highlight the need to modernize the integrated naval weapon system and strengthen regional maritime defense cooperation, along with adopting a multidimensional approach and inter-agency synergy to enhance national maritime security amid the growing complexity of hybrid threats.*

Keywords: *hybrid threats, maritime security, Indonesian Navy posture, national defense*

Abstrak: Perubahan lingkungan strategis global dan regional telah memunculkan ancaman hibrida yang menggabungkan unsur militer dan nonmiliter. Sebagai negara kepulauan dengan posisi geostrategis penting, Indonesia menghadapi kerentanan tinggi terhadap ancaman tersebut, terutama di sektor maritim. Penelitian ini bertujuan menganalisis karakteristik ancaman hibrida yang mempengaruhi keamanan maritim Indonesia serta dampaknya terhadap postur TNI Angkatan Laut. Metode penelitian kualitatif deskriptif melalui analisis konten dokumen strategis, data Global Fire Power, dan literatur akademik, penelitian mengidentifikasi lima bentuk ancaman utama: disinformasi digital, serangan siber, kejahatan lintas negara, infiltrasi ekonomi, dan aksi proksi di perbatasan laut. Hasil menunjukkan perlunya modernisasi sistem senjata armada terpadu dan penguatan kerja sama pertahanan maritim regional, serta penerapan pendekatan multidimensi dan sinergi antarlembaga untuk memperkuat keamanan maritim nasional di tengah kompleksitas ancaman hibrida.

Kata kunci: ancaman hibrida, keamanan maritim, postur TNI Angkatan Laut, pertahanan nasional

PENDAHULUAN

Perubahan lanskap ancaman global selama dekade terakhir menandai pergeseran dari konfrontasi militer tradisional menuju kontestasi yang lebih kompleks dan multidimensi. Konsep *hybrid warfare* menggambarkan kombinasi antara tindakan militer konvensional dan non-konvensional, termasuk operasi siber, kampanye disinformasi, tekanan ekonomi, penggunaan aktor non-negara, dan taktik *gray zone* yang dirancang untuk mencapai tujuan strategis sambil tetap berada di bawah ambang tindakan perang terbuka (Stensrud & Østhagen, 2024; Genini, 2025; Lott, 2022). Menurut Hoffman (2007) perang hibrida merupakan bentuk evolusi konflik modern yang mengintegrasikan instrumen militer dan non-militer dalam spektrum persaingan strategis. Karakter transnasional dan multifaset dari ancaman ini membuat batas antara situasi damai dan konflik semakin kabur, sehingga menuntut pendekatan keamanan yang tidak hanya militer, tetapi juga terintegrasi lintas sektor (Bueger & Liebetrau, 2023; Kismartini et al., 2024).

Posisi geografis Indonesia sebagai negara kepulauan besar menempatkan negara ini pada persimpangan jalur perdagangan maritim dunia. Alur Laut Kepulauan Indonesia (ALKI I–III) merupakan koridor strategis yang menghubungkan Samudra Hindia, Selat Malaka, dan Samudra Pasifik, menjadikan perairan Indonesia sebagai jalur vital bagi arus barang, energi, dan informasi global (Rahayu et al., 2024; Mohsendokht et al., 2024). Kerentanan infrastruktur maritim kritis seperti pelabuhan, kabel bawah laut, sistem navigasi, dan rantai pasok logistik memberi peluang bagi aktor yang memanfaatkan teknik hibrid untuk mengganggu stabilitas ekonomi dan keamanan nasional (Bueger & Liebetrau, 2023; Clavijo Mesa et al., 2024).

Konteks global tersebut tercermin dalam dinamika domestik dan regional Indonesia. Insiden kekerasan di Poso dan Papua menunjukkan penggunaan jaringan lokal dan manipulasi informasi melalui platform digital; sementara di Laut Natuna meningkat aktivitas kapal asing dan tekanan maritim non-kinetik yang memanfaatkan ambiguitas hukum laut. Selain itu, meningkatnya serangan siber terhadap sistem pelabuhan dan logistik maritim memperlihatkan ancaman terhadap infrastruktur *cyber-physical* (Fenton, 2024; Clavijo Mesa et al., 2024). Fenomena-fenomena tersebut menunjukkan bahwa elemen perang hibrida telah menembus domain maritim Indonesia, melibatkan aktor negara dan non-negara dengan intensitas yang kian meningkat (Symes et al., 2024; Liebetrau & Bueger, 2024).

Namun, berbagai penelitian terdahulu umumnya berfokus pada ancaman militer konvensional dan belum mengintegrasikan dimensi ancaman non-militer seperti siber, ekonomi, dan informasi dalam konteks pertahanan maritim Indonesia. Oleh karena itu, masih terdapat kesenjangan konseptual dalam memahami bagaimana ancaman hibrida memengaruhi postur TNI Angkatan Laut secara strategis. Kajian sistematik mengenai bentuk, pola, dan interaksi (nexus) antara berbagai dimensi ancaman hibrida di sektor maritim menjadi penting untuk mengisi kekosongan literatur tersebut dan mendukung perumusan kebijakan pertahanan yang adaptif

Penelitian ini bertujuan untuk menganalisis bentuk-bentuk ancaman hibrida yang mengancam keamanan maritim Indonesia serta menelaah implikasinya terhadap postur dan kebijakan TNI Angkatan Laut. Kebaruan penelitian ini terletak pada integrasi analisis ancaman hibrida lintas dimensi meliputi siber, ekonomi, dan proksi ke dalam evaluasi postur pertahanan laut Indonesia yang belum banyak dikaji secara komprehensif.

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif yang bertujuan menggambarkan secara sistematis bentuk dan karakteristik ancaman hibrida terhadap keamanan maritim Indonesia. Pendekatan ini dipilih karena memungkinkan peneliti memahami fenomena ancaman hibrida yang bersifat kompleks, kontekstual, dan dinamis.

Penelitian ini berorientasi pada analisis mendalam terhadap berbagai sumber data sekunder untuk menafsirkan makna dan hubungan antarkomponen ancaman.

Sumber data utama meliputi Rencana Strategis TNI Angkatan Laut Tahun 2020–2024, Global Fire Power 2023, serta berbagai literatur akademik dan laporan kebijakan yang relevan dengan isu pertahanan maritim dan perang hibrida. Penggunaan data sekunder dipilih karena seluruh informasi strategis terkait postur pertahanan laut dan dinamika ancaman telah terdokumentasi secara resmi dalam sumber otoritatif. Kredibilitas data dijaga melalui seleksi ketat terhadap dokumen yang bersifat valid, resmi, dan mutakhir.

Dalam penelitian ini, peneliti berperan sebagai instrumen utama yang menafsirkan data melalui pembacaan mendalam (close reading) dan pemetaan makna strategis. Data dianalisis menggunakan dua teknik, yakni analisis konten dan analisis tematik. Analisis konten dilakukan dalam tiga tahap: (1) identifikasi unit analisis yang relevan dengan konsep ancaman hibrida, (2) pengkodean dan pengelompokan isi berdasarkan dimensi militer, non-militer, ekonomi, informasi, dan siber, serta (3) penarikan makna kontekstual dari pola yang muncul. Analisis tematik kemudian digunakan untuk menemukan tema-tema utama yang mencerminkan relasi antar kategori dan implikasinya terhadap keamanan laut nasional.

Validitas hasil penelitian melalui triangulasi sumber, yaitu pembandingan antar dokumen strategis, data pertahanan, dan literatur akademik guna memastikan konsistensi dan reliabilitas informasi. Berdasarkan hasil analisis awal, diperoleh sepuluh kategori ancaman hibrida sebagaimana ditunjukkan pada Tabel 1.

Tabel 1. Jenis Ancaman Hibrida

Jenis Ancaman	Deskripsi	Contoh
Ancaman Ideologi	Ancaman yang mengeksploitasi kerentanan dengan menyebarkan ideologi asing yang tidak sesuai dengan kepribadian bangsa. Melemahkan dan mengganggu stabilitas Negara dengan cara Mengubah atau mengganti ideologi dasar negara, Menciptakan konflik internal dan perpecahan sosial, Mengikis kedaulatan negara dari dalam	Penyebaran pahan liberalisme, komunisme, atau ideologi radikal lainnya
Ancaman Militer	Melibatkan penggunaan kekuatan militer secara langsung, seperti serangan konvensional, penyerangan dengan senjata, atau mobilisasi pasukan.	Serangan siber terhadap infrastruktur penting. Penggunaan pasukan reguler untuk tujuan strategis.
Ancaman Siber	Serangan yang dilakukan melalui jaringan komputer dan sistem informasi.	Pencurian data rahasia. Peretasan sistem vital. Penyebaran malware dan virus. Peretasan *situs web* pemerintah, serangan ransomware pada rumah sakit, atau pencurian data kartu kredit.
Ancaman Informasi	Manipulasi informasi dan penyebaran berita bohong untuk mempengaruhi opini publik. Penyebaran informasi palsu atau menyesatkan untuk mempengaruhi opini publik, merusak reputasi, atau mengacaukan situasi	Penyebaran propaganda untuk memicu konflik. Membuat berita palsu untuk merusak reputasi. Mempengaruhi opini publik melalui media sosial. Penyebaran berita bohong tentang pandemi, kampanye propaganda untuk mempengaruhi pemilu, atau penyebaran ujaran kebencian
Ancaman Ekonomi	Penggunaan kekuatan ekonomi untuk mencapai tujuan politik.	Sanksi ekonomi terhadap negara lain. Manipulasi pasar keuangan untuk melemahkan negara lain. Korupsi dan pencucian uang. Embargo minyak, manipulasi nilai tukar mata uang, atau pembatasan akses ke teknologi penting

Kriminalitas Terorganisir	Penggunaan jaringan kriminal untuk melakukan kejahatan transnasional, seperti perdagangan narkoba, perdagangan manusia, atau kejahatan dunia maya	Kartel narkoba yang menggunakan kekerasan untuk mengendalikan wilayah, atau jaringan perdagangan manusia yang mengeksploitasi imigran.
Aksi Proksi	Dukungan rahasia terhadap kelompok pemberontak, milisi, atau organisasi teroris untuk mencapai tujuan politik	Penyediaan senjata dan pelatihan kepada kelompok bersenjata, atau pendanaan untuk kegiatan terorisme
Penggunaan Teknologi	Pemanfaatan teknologi seperti drone, kecerdasan buatan, atau teknologi pengawasan untuk tujuan militer atau non-militer.	Penggunaan drone untuk serangan militer, atau penggunaan kecerdasan buatan untuk memantau aktivitas warga.
Ancaman terhadap Infrastruktur	Serangan terhadap sistem transportasi, energi, air, atau komunikasi yang vital bagi kehidupan masyarakat.	Pengeboman jembatan atau jalur kereta api, serangan terhadap pembangkit listrik, atau gangguan pada sistem komunikasi.

Sumber: olahan peneliti (2025)

Hasil analisis lebih lanjut menunjukkan bahwa tidak seluruh jenis ancaman tersebut memiliki relevansi langsung terhadap sektor maritim. Melalui proses reduksi data, peneliti mengelompokkan ancaman yang paling berpengaruh terhadap keamanan laut Indonesia ke dalam lima kategori utama, yakni ancaman informasi dan siber, ancaman ekonomi, ancaman proksi dan separatis, ancaman kriminalitas terorganisir, serta ancaman terhadap infrastruktur strategis. Hasil tersebut menjadi dasar pembahasan pada bagian berikutnya.

HASIL DAN PEMBAHASAN

a) Klasifikasi Ancaman Hibrida terhadap Keamanan Maritim

Analisis data sekunder menunjukkan bahwa ancaman hibrida terhadap keamanan maritim Indonesia dapat diklasifikasikan ke dalam lima bentuk utama: ancaman informasi dan siber, ancaman ekonomi, ancaman proksi dan separatis, ancaman kriminalitas terorganisir, serta ancaman terhadap infrastruktur strategis. Ancaman informasi dan siber tercermin melalui serangan terhadap sistem komunikasi militer, penyebaran disinformasi maritim, serta propaganda digital yang bertujuan melemahkan legitimasi pemerintah dan menciptakan instabilitas persepsi publik (Liebetrau & Bueger, 2024; Clavijo Mesa et al., 2024).

Serangan siber pada infrastruktur kelautan nasional juga meningkat seiring digitalisasi sistem navigasi dan logistik maritim (Mohsendokht et al., 2024). Ancaman ekonomi muncul dalam bentuk manipulasi pasar energi, eksploitasi sumber daya laut secara ilegal, serta tekanan ekonomi global yang berdampak pada ketahanan maritim nasional (Rahayu et al., 2024). Sementara itu, ancaman proksi dan separatis berkembang melalui dukungan eksternal terhadap kelompok bersenjata dan gerakan separatis di wilayah maritim seperti Papua dan Natuna (Mandaku & Samad, 2022). Ancaman kriminalitas terorganisir mencakup aktivitas penyelundupan, perdagangan manusia, narkotika laut, serta perompakan di jalur perairan strategis Indonesia (Bueger & Liebetrau, 2023). Adapun ancaman terhadap infrastruktur maritim semakin kompleks, melibatkan sabotase pelabuhan, gangguan sistem komunikasi laut, serta potensi serangan terhadap fasilitas energi dan pangkalan angkatan laut (Malik et al., 2024; Abyasa et al., 2025).

Beragam ancaman tersebut menunjukkan bahwa karakter perang hibrida telah menembus batas-batas fisik wilayah, sehingga keamanan maritim tidak lagi dapat dipandang semata-mata sebagai domain militer, melainkan sebagai sistem multidimensi yang mencakup aspek teknologi, ekonomi, sosial, dan geopolitik (Stensrud & Østhagen, 2024; Sarjito, 2024). Temuan ini memperkuat teori hybrid warfare (Hoffman, 2007) yang menekankan bahwa konvergensi antara domain fisik dan digital merupakan bentuk evolusi konflik modern. Dalam konteks Indonesia, dinamika ini sesuai dengan konsep maritime security governance yang menuntut koordinasi antarlembaga dalam menghadapi ancaman

non-tradisional (Bueger & Liebetrau, 2023). Klasifikasi tersebut menjadi dasar analisis lebih lanjut mengenai implikasi strategisnya terhadap postur pertahanan laut Indonesia.

b) Implikasi terhadap Postur TNI Angkatan Laut

Hasil analisis menunjukkan bahwa munculnya ancaman hibrida menuntut penyesuaian postur TNI Angkatan Laut (TNI AL) pada empat dimensi strategis utama: teknologi, sumber daya manusia (SDM), operasional, dan diplomasi pertahanan. Dari sisi teknologi, terdapat kebutuhan mendesak untuk modernisasi Sistem Senjata Armada Terpadu (SSAT) dan penguatan sistem pertahanan siber serta integrasi maritime surveillance system. Penguatan kemampuan cyber defense dan sistem deteksi dini menjadi elemen kunci dalam merespons ancaman non-konvensional secara real-time. Pada dimensi SDM, peningkatan kapasitas intelijen maritim, literasi digital militer, serta pelatihan deteksi ancaman informasi menjadi prioritas.

Dari perspektif operasional, sinergi antara TNI AL, Bakamla, Kementerian Kelautan dan Perikanan (KKP), dan lembaga intelijen perlu diperkuat untuk membangun pola operasi bersama yang adaptif terhadap ancaman multidomain. Dimensi diplomatik menekankan pentingnya kerja sama pertahanan laut regional melalui ASEAN Defence Ministers' Meeting Plus (ADMM+) dan Indo-Pacific Maritime Cooperation untuk memperkuat kolektivitas keamanan Kawasan. Pendekatan komprehensif ini sejalan dengan konsep smart defense dan integrated maritime security (Lott, 2022; Genini, 2025). Pendekatan serupa telah diterapkan di Singapura dan Filipina melalui strategi *whole-of-government*, yang menekankan interoperabilitas lintas lembaga dalam menghadapi ancaman lintas. Berdasarkan evaluasi atas empat dimensi strategis tersebut, disusun arah penguatan postur yang relevan dengan konteks ancaman hibrida di kawasan maritim Indonesia.

c) Arah Strategi Penguatan Postur

Berdasarkan hasil analisis, arah strategi penguatan postur TNI AL difokuskan pada tiga langkah utama. Pertama, optimalisasi pangkalan di kawasan perbatasan laut seperti Natuna, Bitung, dan Saumlaki guna meningkatkan efek tangkal (*deterrence effect*) terhadap ancaman lintas batas. Kedua, integrasi pusat data intelijen maritim berbasis digital sebagai sarana pertukaran informasi real-time antara matra laut, udara, dan lembaga keamanan sipil. Ketiga, revitalisasi latihan perang laut gabungan dan patroli multinasional, termasuk keterlibatan dalam latihan bersama ASEAN, India, dan Australia untuk memperkuat interoperabilitas dan kesiapan menghadapi perang hibrida.

Penerapan strategi ini perlu diiringi oleh reformasi kelembagaan, peningkatan efisiensi logistik, serta investasi berkelanjutan dalam riset dan teknologi pertahanan maritim. Namun demikian, implementasi strategi tersebut dihadapkan pada tantangan seperti keterbatasan anggaran, kesenjangan teknologi, serta koordinasi lintas lembaga yang masih perlu diperkuat. Rekomendasi penelitian ini melengkapi arah kebijakan Renstra TNI AL 2020–2024 dengan menekankan urgensi digitalisasi sistem intelijen maritim dan peningkatan interoperabilitas lintas matra sebagai elemen utama pertahanan adaptif di era hibrida.

KESIMPULAN

Penelitian ini menegaskan bahwa ancaman hibrida terhadap keamanan maritim Indonesia telah berkembang menjadi ancaman multidimensi yang melibatkan aspek informasi, siber, ekonomi, proksi, kriminalitas lintas negara, dan infrastruktur strategis. Temuan ini menunjukkan bahwa bentuk ancaman modern tidak lagi terbatas pada domain militer, melainkan meluas ke ranah ekonomi dan digital yang saling berinteraksi. Dalam konteks tersebut, TNI Angkatan Laut perlu menyesuaikan posturnya melalui modernisasi sistem senjata armada terpadu, penguatan pertahanan siber, serta peningkatan kemampuan intelijen dan

diplomasi maritim. Kebaruan penelitian ini terletak pada integrasi analisis ancaman multidomain dalam sektor maritim Indonesia serta formulasi arah strategi penguatan postur pertahanan laut yang responsif terhadap karakter perang hibrida. Upaya penguatan tersebut harus didukung oleh sinergi antarlembaga nasional, peningkatan interoperabilitas lintas matra, serta kerja sama pertahanan regional di bawah kerangka ASEAN dan Indo-Pacific. Dengan demikian, penguatan postur TNI AL bukan hanya menjadi keharusan pertahanan, tetapi juga bagian dari strategi diplomasi maritim untuk membangun keamanan nasional yang tangguh, adaptif, dan berkelanjutan di tengah dinamika ancaman global.

REFERENSI

Abyasa, K. P., Sari, D. S., & Konety, N. (2025). Strategi Pengamanan Laut Indonesia Terhadap Arus Pengungsi Ilegal. *Aliansi : Jurnal Politik, Keamanan Dan Hubungan Internasional*, *3*(3), 141–149. https://doi.org/10.24198/aliansi.v3i3.60182

Bueger, C., & Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy*, *155*, 105772. https://doi.org/https://doi.org/10.1016/j.marpol.2023.105772

Clavijo Mesa, M. V, Patino-Rodriguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. In *Information* (Vol. 15, Issue 11). https://doi.org/10.3390/info15110710

Fenton, A. J. (2024). Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore. In *Journal of Marine Science and Engineering* (Vol. 12, Issue 3). https://doi.org/10.3390/jmse12030510

Genini, D. (2025). Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*, *33*(2), 122–149. https://doi.org/https://doi.org/10.1177/2336825X251322719

Hoffman, F. (2007). Conflict in The 21st Century: The Rise of Hybrid Wars. *Potomac Institute for Policy Studies*.

Kismartini, K., Yusuf, I., Sabilla, K., & Roziqin, A. (2024). A bibliometric analysis of maritime security policy: Research trends and future agenda. *Heliyon*, *10*, e28988. https://doi.org/10.1016/j.heliyon.2024.e28988

Liebetrau, T., & Bueger, C. (2024). Advancing coordination in critical maritime infrastructure protection: Lessons from maritime piracy and cybersecurity. *International Journal of Critical Infrastructure Protection*, *46*, 100683. https://doi.org/https://doi.org/10.1016/j.ijcip.2024.100683

Lott, A. (2022). *Hybrid Threats and the Law of the Sea*. Brill. https://doi.org/10.1163/9789004509368

Malik, K., Putra, I., Darwan, D., Wiratama, A., Setiawan, F., & Saputro, B. (2024). Studi Karakteristik Pasut, Arus Pasut, dan Gelombang pada Perencanaan Pembangunan Pangkalan TNI AL Saumlaki Menggunakan Pemodelan Numerik. *Jurnal Chart Datum*, *9*(2), 123–134. https://doi.org/10.37875/chartdatum.v9i2.293

Mandaku, H., & Samad, M. Y. (2022). POTENSI ANCAMAN PERANG HIBRIDA DI INDONESIA PADA TAHUN 2023: AKTOR, METODE, DAMPAK. *Jurnal Cendekia Waskita*, *6*(2), 184–194.

Mohsendokht, M., Li, H., Kontovas, C., Chang, C.-H., Qu, Z., & Yang, Z. (2024). Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. *Ocean Engineering*, *312*, 119078. https://doi.org/https://doi.org/10.1016/j.oceaneng.2024.119078

Rahayu, L., Busscher, T., Tillema, T., & Woltjer, J. (2024). Maritime transport governance challenges in the Global South. *Marine Policy*, *163*, 106147.

https://doi.org/https://doi.org/10.1016/j.marpol.2024.106147
Sarjito, A. (2024). Peran Intelijen Melalui Perumusan Kebijakan Pertahanan Negara dalam Perang Hibrida. *PANDITA: Interdisciplinary Journal of Public Affairs*, *7*(1), 74–88. https://doi.org/https://doi.org/10.61332/ijpa.v7i1.152
Stensrud, C. J., & Østhagen, A. (2024). Hybrid Warfare at Sea? Russia, Svalbard and the Arctic. *Scandinavian Journal of Military Studies*, *7*(1), 111–130. https://doi.org/10.31374/sjms.233
Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). Cyberattacks on the Maritime Sector: A Literature Review. *Journal of Marine Science and Application*, *23*. https://doi.org/10.1007/s11804-024-00443-0