

Artificial Intelligence for Maritime Security Resilience

Lukman Yudho Prakoso^{1*}, M. Risahdi², Mugi Suroño Selamat³

Universitas Pertahanan RI

Corresponding Author: Lukman Yudho Prakoso lukman.prakoso@idu.ac.id

ARTICLE INFO

Keywords: Artificial Intelligence, Security, Maritime

Received : 02 July 2025

Revised : 25 July 2025

Accepted: 28 August 2025

©2025 Prakoso, Risahdi, Selamat: This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

This study discusses the application of Artificial Intelligence (AI) as a key strategy in strengthening Indonesia's maritime security resilience. By utilizing real-time data analysis from satellites, radar, AIS, and underwater sensors, AI is expected to improve early detection capabilities, threat prediction, and patrol optimization. This study uses a qualitative descriptive approach to analyze global, regional, and national maritime security conditions, and identifies challenges to AI implementation in Indonesia. The analysis is conducted using Lukman Yudho Prakoso's policy implementation theory and Clausewitz's strategy theory to formulate an integrative, interactive, transparent, and accountable maritime security strategy. The results show that the systematic application of AI can improve the effectiveness of maritime surveillance, threat response, and cross-agency and regional cooperation.

Artificial Intelligence Untuk Resilensi Keamanan Maritim

Lukman Yudho Prakoso^{1*}, M. Risahdi², Mugi Suroono Selamat³
Universitas Pertahanan RI

Corresponding Author: Lukman Yudho Prakoso lukman.prakoso@idu.ac.id

ARTICLE INFO

Kata Kunci: Artificial, Intelligence, Keamanan, Maritim

Received : 02 Juli 2025

Revised : 25 Juli 2025

Accepted: 28 Agustus 2025

©2025 Prakoso, Risahdi, Selamat: This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRAK

Penelitian ini membahas penerapan Artificial Intelligence (AI) sebagai strategi utama dalam memperkuat resiliensi keamanan maritim Indonesia. Dengan memanfaatkan analisis data real-time dari satelit, radar, AIS, dan sensor bawah laut, AI diharapkan mampu meningkatkan kemampuan deteksi dini, prediksi ancaman, serta optimalisasi patroli. Studi ini menggunakan pendekatan deskriptif kualitatif untuk menganalisis kondisi keamanan maritim global, regional, dan nasional, serta mengidentifikasi tantangan implementasi AI di Indonesia. Analisis dilakukan menggunakan teori implementasi kebijakan Lukman Yudho Prakoso dan teori strategi Clausewitz untuk merumuskan strategi keamanan maritim yang integratif, interaktif, transparan, dan akuntabel. Hasil penelitian menunjukkan bahwa penerapan AI secara sistematis dapat meningkatkan efektivitas pengawasan laut, respons ancaman, serta kerja sama lintas instansi dan regional.

PENDAHULUAN

Keamanan maritim global mengalami dinamika yang semakin kompleks. Laporan International Maritime Bureau mencatat adanya 120 insiden pembajakan pada 2023, dengan tren penculikan awak kapal yang meningkat (International Maritime Bureau, 2023). Fenomena shadow fleet – diperkirakan mencapai 600 kapal – beroperasi dengan mematikan AIS (Automatic Identification System) dan memalsukan bendera kapal untuk menghindari sanksi (Milne, 2025). Serangan siber terhadap infrastruktur bawah laut dan sistem navigasi maritim juga meningkat, mendorong NATO untuk meluncurkan operasi Baltic Sentry guna melindungi pipa dan kabel bawah laut (Strobel, 2025). Regional. Di kawasan Asia, serangan kelompok Houthi terhadap kapal komersial di Laut Merah memaksa lebih dari 2.000 kapal mengubah rute pelayaran, meningkatkan biaya logistik dan risiko rantai pasok (Center for Strategic and International Studies [CSIS], 2024). Selat Malaka, sebagai salah satu choke point strategis dunia, menjadi area dengan risiko tinggi perompakan dan penyelundupan (Asian Development Bank, 2024).

Nasional. Indonesia sebagai negara kepulauan terbesar di dunia menghadapi tantangan serius di Zona Ekonomi Eksklusif (ZEE), termasuk illegal, unreported, and unregulated (IUU) fishing, penyelundupan narkoba, dan pelanggaran wilayah oleh kapal asing. Sistem pemantauan laut nasional masih bergantung pada patroli konvensional dan radar terbatas, sementara penerapan AI untuk pengawasan laut masih minim (Badan Keamanan Laut Republik Indonesia, 2024).

Ancaman Keamanan Maritim & Minimnya Sistem Berbasis AI

Ancaman maritim saat ini meliputi:

- Piracy – 120 insiden pada 2023, dengan kecenderungan peningkatan aksi kekerasan (International Maritime Bureau, 2023).
- Cyber threats – serangan terhadap pelabuhan dan sistem AIS meningkat 38% dalam setahun, dan 60% pelabuhan besar belum memiliki pertahanan siber memadai (Fernandez et al., 2023).
- Shadow fleets – digunakan untuk perdagangan ilegal dan penghindaran sanksi (Milne, 2025).
- Gangguan rantai pasok – konflik Laut Merah mengakibatkan kerugian miliaran dolar per bulan akibat rerouting kapal (CSIS, 2024).

Sistem keamanan maritim konvensional tidak mampu memberikan respons cepat. Keterlambatan deteksi dan lemahnya koordinasi antarinstansi menjadi celah yang dapat dimanfaatkan aktor kriminal maupun negara yang bermusuhan.

Pandangan Ahli dan Teori Keamanan Maritim yang Ideal

Menurut Johnson (2024), penerapan AI di sektor maritim memungkinkan identifikasi kapal gelap (dark ships), deteksi IUU fishing, dan pemantauan pelabuhan secara proaktif melalui deteksi anomali berbasis machine learning. Saildrone telah mengembangkan kapal tanpa awak bertenaga AI yang dapat

beroperasi terus-menerus untuk memantau ancaman seperti penyelundupan atau sabotase kabel bawah laut (Sherwood, 2025).

Di Eropa, Common Information Sharing Environment (CISE) menjadi model berbagi data terintegrasi antara lebih dari 300 otoritas maritim untuk meningkatkan kesadaran situasional dan respons bersama (European Maritime Safety Agency, 2023). Model serupa dapat diadaptasi oleh Indonesia untuk mengoptimalkan koordinasi lintas instansi.

Urgensi dan Kebutuhan Penelitian

Dengan ancaman fisik dan siber yang semakin kompleks, penerapan AI dalam keamanan maritim menjadi kebutuhan mendesak. AI mampu memproses data multi-sumber (citra satelit, sensor AIS, drone, dan intelijen) secara real-time untuk mendeteksi aktivitas mencurigakan sebelum eskalasi terjadi (Johnson, 2024).

Penelitian ini diperlukan untuk, Merumuskan strategi keamanan maritim berbasis AI yang sesuai konteks Indonesia, Meningkatkan efektivitas pengawasan laut dan respons terhadap ancaman, Memperkuat interoperabilitas antarinstansi dan kerja sama regional.

TINJAUAN PUSTAKA

Artificial Intelligence (AI) dapat meningkatkan resiliensi keamanan maritim melalui kemampuan deteksi dini, analisis anomali, dan respons cepat terhadap ancaman laut (Johnson, 2024). Penelitian ini memanfaatkan teori implementasi kebijakan publik oleh Lukman Yudho Prakoso, yang menggagas faktor-faktor IITCA – Integratif, Interaktif, Transparan, Kontrol, Akuntabel – sebagai kerangka evaluasi implementasi keamanan maritim berbasis AI dalam konteks Indonesia (Prakoso, 2021). Selanjutnya, teori strategi Clausewitz – dengan konsep *ends, ways, dan means* – digunakan untuk menyelaraskan tujuan strategis keamanan, metode implementasi, dan sumber daya tersedia (Howard & Paret, 1984). Pendekatan ganda ini dirancang untuk menghasilkan strategi keamanan maritim berbasis AI yang efektif, akuntabel, dan adaptif terhadap tantangan lokal serta memperkuat interoperabilitas antarinstansi serta kerja sama regional.

METODOLOGI

Penelitian ini menggunakan metode deskriptif kualitatif sebagaimana dijelaskan Creswell (2018), yang bertujuan memahami fenomena secara mendalam melalui pengumpulan dan analisis data non-numerik. Pendekatan ini dipilih untuk menggali secara komprehensif implementasi Artificial Intelligence (AI) dalam memperkuat resiliensi keamanan maritim Indonesia. Data dikumpulkan melalui studi literatur, wawancara mendalam dengan pakar maritim, dan analisis dokumen kebijakan. Analisis dilakukan dengan mengidentifikasi pola, tema, dan keterkaitan antara penerapan AI dengan faktor-faktor strategis keamanan maritim. Metode ini memungkinkan peneliti mengaitkan temuan dengan teori implementasi kebijakan Lukman Yudho Prakoso dan teori strategi Clausewitz, guna menghasilkan strategi keamanan maritim yang relevan dan adaptif terhadap dinamika ancaman.

HASIL PENELITIAN

Analisis data menunjukkan bahwa ancaman maritim bersifat multi-dimensi—fisik, siber, dan politik—dan berdampak langsung pada keamanan pasokan global dan kedaulatan negara. International Maritime Bureau (IMB) melaporkan 120 insiden pembajakan dan perampokan bersenjata terhadap kapal pada 2023 (International Maritime Bureau, 2024). Konflik di Laut Merah/selat Suez memaksa ratusan kapal merutek ulang, memperpanjang waktu perjalanan hingga 10-14 hari dan menambah biaya operasional serta premi asuransi (Reuters, 2023; CSIS, 2024). Fenomena shadow fleet—ratusan tanker yang berpindah bendera dan mematikan AIS untuk mengelabui sanksi—menambah kompleksitas pengawasan maritim global (AP, 2025; Milne, 2025). Di ranah siber, laporan Coast Guard menunjukkan puluhan insiden siber yang dilaporkan ke unit-unit tertentu pada 2024, sementara survei industri memperingatkan bahwa lebih dari sepertiga profesional maritim memperkirakan ancaman siber meningkat (U.S. Coast Guard, 2024; DNV, 2024).

Di tingkat nasional, Indonesia menghadapi IUU fishing, penyelundupan, dan pelanggaran ZEE yang terus terjadi. Badan Keamanan Laut (Bakamla) mencatat berbagai insiden dan merilis laporan kinerja tahunan yang menegaskan frekuensi kejadian keamanan laut sepanjang 2023 (Bakamla RI, 2023). Organisasi pemantau seperti IOJI dan analisis IUU Fishing Risk Index juga mendeteksi kapal-kapal asing beraktivitas mencurigakan di perairan timur Indonesia (IOJI, 2024; IUU Fishing Risk Index, 2023). Pemerintah melaporkan upaya penegakan termasuk strategi Bali terhadap IUU fishing dan klaim pencegahan kerugian ekonomi (KKP; moderndiplomacy, 2025).

Analisis menurut faktor implementasi kebijakan: Integratif, Interaktif, Transparan, Akuntabel

1. Integratif

Temuan menunjukkan rendahnya integrasi sistem informasi maritim saat ini. Banyak data relevan—citra satelit, sinyal AIS, laporan patroli, intelijen siber—masih terfragmentasi antar-lembaga nasional dan regional. Contoh positif internasional, seperti platform berbagi data (CISE di Eropa) dan sistem peringatan dini berbasis AI (VIEWS/CEWS) memperlihatkan manfaat integrasi data lintas aktor untuk deteksi dini (European Maritime initiatives; ACCORD, 2022). Di Indonesia, meskipun Bakamla, KKP, TNI-AL, dan instansi lain memiliki kapabilitas masing-masing, belum ada integrasi nasional yang memanfaatkan AI untuk menyatukan dan menganalisis multi-sumber data secara real-time—sebuah gap yang mengurangi efektivitas respons.

2. Interaktif

Interaktivitas berarti kemampuan sistem untuk mendorong kolaborasi operasional dan intelijen antar-pemangku kepentingan. Di skala global, model AI untuk simulasi skenario dan pemetaan risiko (mis. digital twin) telah meningkatkan dialog antar-negara dan antar-lembaga (UNDP/CulturePulse; Heaven, 2023). Penelitian ini menemukan interaktivitas yang terbatas di tingkat nasional—mis. keterbatasan akses bagi nelayan lokal, LSM lingkungan, dan otoritas daerah untuk memberi input data

yang kemudian dianalisis oleh sistem pusat. Tanpa mekanisme interaktif, AI berisiko menjadi alat top-down yang miskin konteks lokal.

3. **Transparan**

Transparansi algoritmik dan proses analitik esensial untuk membangun kepercayaan. Internasional menampilkan inisiatif audit algoritma dan kebijakan keterbukaan untuk sistem pengawasan (European Commission; ECAT). Namun di banyak kasus – termasuk pengawasan pelabuhan dan deteksi kapal gelap – algoritma dan data tetap “kotak hitam” bagi publik dan aktor non-teknis. Di Indonesia, penggunaan teknologi pengawasan yang tidak transparan dapat memicu resistensi publik dan menurunkan legitimasi tindakan penegakan.

4. **Akuntabel**

Akuntabilitas mensyaratkan jejak keputusan, mekanisme audit, dan sanksi atas penyalahgunaan. Contoh global menggabungkan jejak audit dan kebijakan human-in-the-loop untuk memastikan keputusan kritis tetap di bawah kontrol manusia (Devitt et al., 2021). Temuan lapangan menegaskan bahwa Indonesia belum memiliki mekanisme audit teknologi maritim yang baku – sehingga tanggung jawab dan hak peninjauan atas keputusan yang dihasilkan sistem masih lemah.

Implikasi temuan

Kesenjangan integrasi, interaktivitas, transparansi, dan akuntabilitas memperkecil efektivitas respon maritim terhadap ancaman yang cepat dan multi-dimensi. Sementara AI terbukti mampu meningkatkan deteksi anomali (kapal tanpa AIS, pola penangkapan IUU, anomali jaringan siber) dalam studi internasional, penerapan di Indonesia masih terbatas oleh fragmentasi data, keterbatasan sumber daya manusia, dan ketiadaan kerangka kebijakan AI maritim yang komprehensif.

PEMBAHASAN

1. Strategi Keamanan Maritim Berbasis AI yang Sesuai Konteks Indonesia (Teori Clausewitz: Ends, Ways, Means)

Penggunaan kerangka strategi Clausewitz yang memisahkan tujuan (Ends), cara (Ways), dan sumber daya (Means) memberikan landasan analitis untuk merancang strategi keamanan maritim berbasis AI yang realistis, terukur, dan adaptif.

Ends (Tujuan Strategis)

Dalam konteks Indonesia, ends utama adalah mewujudkan keamanan maritim yang mampu:

- Menjamin kedaulatan wilayah laut dan Zona Ekonomi Eksklusif (ZEE) dari ancaman militer, kejahatan lintas batas, dan pelanggaran hukum internasional.
- Mengamankan jalur komunikasi laut (Sea Lines of Communication/SLOC) yang krusial bagi perdagangan domestik dan global.

- Menekan kerugian ekonomi akibat Illegal, Unreported, and Unregulated (IUU) fishing, penyelundupan, dan pembajakan.
- Mempertahankan stabilitas ekosistem laut untuk keberlanjutan ekonomi biru (blue economy).

Menurut laporan Kementerian Kelautan dan Perikanan (KKP), IUU fishing menimbulkan potensi kerugian ekonomi mencapai Rp 101 triliun per tahun (KKP, 2024). Di sisi lain, Bakamla RI (2023) melaporkan adanya puluhan insiden pelanggaran wilayah oleh kapal asing setiap tahunnya, khususnya di Laut Natuna Utara. Secara global, International Maritime Bureau (2024) mencatat 120 insiden pembajakan dan perampokan bersenjata terhadap kapal pada 2023. Data ini menunjukkan bahwa tujuan strategis AI dalam keamanan maritim Indonesia harus berorientasi pada pencegahan, deteksi dini, dan respons cepat terhadap ancaman multiform.

Ways (Konsep dan Metode)

Penerapan AI dalam keamanan maritim dapat diwujudkan melalui beberapa metode inti:

- Fusi Data Multi-Sumber: Mengintegrasikan Automatic Identification System (AIS), citra satelit (SAR & optik), data sonar, dan intelijen siber dalam satu platform berbasis AI.
- Contoh: Global Fishing Watch dan sistem deteksi kapal gelap menggunakan machine learning untuk mendeteksi pola pergerakan abnormal (Kroodsma et al., 2018).
- Prediksi Perilaku dan Anomali: Model AI dapat mempelajari pola navigasi normal dan menandai perilaku mencurigakan, seperti kapal yang mematikan AIS di wilayah rawan (Milne, 2025).
- Sistem Respons Adaptif: AI mendukung penentuan prioritas patroli berdasarkan skor risiko dinamis, sehingga alokasi sumber daya lebih efisien.
- Penggunaan Digital Twin Maritime: Membuat model virtual perairan Indonesia yang diperbarui secara real-time untuk simulasi skenario ancaman dan mitigasi.
- Metode-metode ini memungkinkan transformasi dari pendekatan reactive menjadi proactive security yang sesuai dengan tantangan keamanan maritim modern.

Means (Sumber Daya)

Keberhasilan strategi memerlukan:

- Infrastruktur teknologi: Server berkapasitas tinggi, jaringan komunikasi laut, satelit nasional, dan sensor maritim.
- Sumber daya manusia: Operator, analis data, dan teknisi AI dengan kompetensi maritim.
- Kerangka regulasi: Standar penggunaan AI di sektor keamanan, termasuk perlindungan data dan privasi.

- Dukungan anggaran: Investasi jangka panjang dalam riset dan pengadaan teknologi.
- Pengalaman Singapura dan Jepang menunjukkan bahwa investasi awal pada infrastruktur pengawasan berbasis AI menghasilkan penghematan biaya patroli hingga 20–30% serta meningkatkan deteksi pelanggaran hingga dua kali lipat (JICA, 2023).

2. Meningkatkan Efektivitas Pengawasan Laut dan Respons terhadap Ancaman

Pengawasan laut yang efektif di Indonesia memerlukan perpaduan antara kemampuan deteksi dini, prediksi risiko, dan respons terkoordinasi. AI berperan pada semua tahap ini.

Efektivitas Deteksi

Sistem AI mampu memproses big data dari berbagai sensor untuk mendeteksi kapal yang mematikan AIS (dark ships), pola penangkapan ikan ilegal, hingga intrusi di area terlarang. Misalnya, analisis berbasis AI oleh IOJI (2024) berhasil mengidentifikasi aktivitas kapal asing di Laut Arafura dengan memanfaatkan citra satelit komersial. Deteksi ini sebelumnya sulit dilakukan dengan patroli manual mengingat luasnya wilayah laut Indonesia (6,4 juta km²).

Di tingkat global, algoritma deep learning yang dioperasikan oleh European Maritime Safety Agency (EMSA) mampu mengidentifikasi potensi polusi minyak dari citra radar Sentinel-1 dengan akurasi >85% (EMSA, 2022). Model serupa dapat diadaptasi untuk deteksi penangkapan ikan ilegal dan tumpahan limbah di perairan Indonesia.

Efektivitas Respons

AI dapat mempercepat proses pengambilan keputusan dengan:

- Memberikan real-time threat assessment kepada pusat komando.
- Mengoptimalkan rute patroli kapal atau UAV untuk mengejar target.
- Menyediakan rekomendasi taktis berbasis predictive analytics.
- Studi Devitt et al. (2021) menegaskan bahwa AI yang dipadukan dengan human-in-the-loop menghasilkan keputusan yang lebih cepat tanpa mengorbankan akurasi operasional.

Pengurangan Waktu Respon

Saat ini, banyak insiden di laut yang memerlukan waktu respons >12 jam sejak deteksi awal. Dengan integrasi AI, waktu ini dapat dipangkas menjadi <4 jam, sebagaimana dibuktikan oleh sistem pengawasan pantai Korea Selatan (KCG, 2022).

3. Memperkuat Interoperabilitas Antarinstansi dan Kerja Sama Regional Tantangan Interoperabilitas

Salah satu hambatan utama keamanan maritim Indonesia adalah fragmentasi data antar-lembaga: TNI AL, Bakamla, KKP, Kementerian Perhubungan, dan Kepolisian Laut. Data disimpan dalam format yang berbeda,

dengan tingkat akses dan prosedur berbagi informasi yang bervariasi. Kondisi ini memperlambat koordinasi dalam merespons ancaman lintas sektor.

Peran AI dalam Interoperabilitas

AI memungkinkan:

- Platform integrasi nasional: Menggabungkan data maritim dari semua instansi dalam National Maritime AI Hub yang dilengkapi modul analitik bersama.
- Standarisasi protokol data: Menggunakan format terbuka (open standards) untuk memudahkan pertukaran data antarinstansi dan mitra internasional.
- Analisis multi-bahasa dan multi-format: AI dapat menerjemahkan dokumen operasional, log komunikasi, dan data teknis dari berbagai sumber secara otomatis.

Kerja Sama Regional

Kerja sama maritim di ASEAN, khususnya di Selat Malaka dan Laut Cina Selatan, membutuhkan interoperabilitas lintas negara. Inisiatif seperti Information Fusion Centre (IFC) di Singapura menunjukkan bahwa platform berbagi informasi real-time dapat menekan jumlah insiden perompakan hingga 50% dalam satu dekade terakhir (IFC, 2022).

Integrasi AI dalam kerja sama regional dapat memperluas kapasitas ini melalui:

- Prediksi pola pergerakan kapal lintas ZEE negara ASEAN.
- Deteksi jaringan kriminal lintas negara berdasarkan data pelabuhan dan intelijen keuangan.
- Dukungan koordinasi patroli gabungan melalui simulasi rute optimal.

Contoh Implementasi

Proyek SeaVision yang dikembangkan oleh AS dan diadopsi di beberapa negara Asia Tenggara sudah menggunakan AI untuk menggabungkan data maritim dan menyediakan gambaran situasional (maritime situational awareness) yang komprehensif. Indonesia berpotensi memperluas partisipasi dan adaptasi platform ini dengan penyesuaian konteks hukum dan operasional domestik.

4. Integrasi Ketiga Rumusan Masalah dalam Strategi Nasional AI Maritim

Ketiga fokus penelitian – perumusan strategi AI maritim sesuai konteks Indonesia, peningkatan efektivitas pengawasan, dan penguatan interoperabilitas – harus dilihat sebagai satu ekosistem strategi. Clausewitz menekankan bahwa keberhasilan strategi bergantung pada kesinambungan antara ends, ways, dan means. Dalam konteks ini:

- Ends: Kedaulatan, keamanan ekonomi, dan stabilitas ekosistem laut.
- Ways: Integrasi teknologi AI untuk deteksi, prediksi, dan respons.
- Means: Infrastruktur teknologi, SDM, regulasi, dan kerja sama regional.

Pendekatan integratif ini sejalan dengan tren global di mana AI tidak hanya dilihat sebagai teknologi, tetapi sebagai force multiplier dalam kerangka keamanan maritim yang terukur, kolaboratif, dan berkelanjutan.

KESIMPULAN DAN REKOMENDASI

Kesimpulan:

Artificial Intelligence (AI) memiliki potensi signifikan dalam memperkuat resiliensi keamanan maritim Indonesia. Melalui kemampuan deteksi dini, analisis data real-time, dan prediksi ancaman, AI dapat meningkatkan efektivitas pengawasan laut, mempercepat respons, serta meminimalkan risiko gangguan keamanan. Penerapan AI juga mendukung transparansi, akuntabilitas, dan koordinasi antarinstansi, sekaligus memperkuat posisi Indonesia di kancah keamanan maritim regional.

Rekomendasi:

Pemerintah perlu mempercepat integrasi AI ke dalam sistem keamanan maritim nasional, memperkuat infrastruktur teknologi, dan meningkatkan kapasitas SDM. Diperlukan pula regulasi yang mendukung pemanfaatan AI secara efektif serta kerja sama internasional untuk berbagi data dan teknologi. Pendekatan kolaboratif menjadi kunci membangun sistem keamanan laut yang adaptif dan tangguh.

PENELITIAN LANJUTAN

Penelitian lanjutan terkait Artificial Intelligence untuk Resiliensi Keamanan Maritim dapat difokuskan pada pengembangan model AI prediktif yang mampu mengantisipasi ancaman sebelum terjadi, termasuk serangan siber terhadap infrastruktur maritim. Kajian juga perlu diarahkan pada integrasi AI dengan teknologi drone laut dan udara untuk patroli otonom, serta sistem komunikasi lintas instansi yang aman. Selain itu, penelitian mendalam tentang etika, privasi data, dan regulasi pemanfaatan AI di sektor maritim menjadi penting untuk memastikan penerapannya sesuai hukum internasional dan kepentingan nasional, sehingga menghasilkan sistem keamanan laut yang lebih proaktif, transparan, dan berkelanjutan.

UCAPAN TERIMA KASIH

Ucapan terima kasih disampaikan kepada Universitas Pertahanan RI, PT. Intek, dan PT. Spasi atas dukungan, kolaborasi, serta kontribusinya dalam penelitian lanjutan ini. Semoga kerja sama ini terus berlanjut demi kemajuan teknologi dan penguatan resiliensi keamanan maritim Indonesia berbasis Artificial Intelligence.

DAFTAR PUSTAKA

- ACCORD. (2022). The role of artificial intelligence in conflict prevention and management in Africa. African Centre for the Constructive Resolution of Disputes. <https://www.accord.org.za/analysis/the-role-of-artificial-intelligence-in-conflict-prevention-and-management-in-africa/>
- AP News. (2025). Shadow fleet of tankers keeps Russia's oil money flowing despite Western sanctions. Associated Press. <https://apnews.com/article/76b66900d599d6e49692643674907fc0>
- Asian Development Bank. (2024). Maritime security challenges in Southeast Asia. <https://www.adb.org>
- Badan Keamanan Laut Republik Indonesia. (2024). Laporan tahunan keamanan laut 2024. Bakamla RI.
- Bakamla RI. (2023). Laporan kinerja 2023. Badan Keamanan Laut Republik Indonesia. <https://bakamla.go.id>
- Center for Strategic and International Studies. (2024). State of maritime supply chain threats. CSIS. <https://www.csis.org>
- CSIS. (2024). The global economic consequences of the attacks on Red Sea shipping lanes. Center for Strategic and International Studies. <https://www.csis.org/analysis/global-economic-consequences-attacks-red-sea-shipping-lanes>
- Devitt, S. K., Scholz, J., Schless, T., & Lewis, L. (2021). Developing a trusted human-AI network for humanitarian benefit. arXiv. <https://arxiv.org/abs/2112.11191>
- Devitt, S. K., Scholz, J., Schless, T., & Lewis, L. (2021). Developing a trusted human-AI network for humanitarian benefit. arXiv. <https://arxiv.org/abs/2112.11191>
- DNV. (2024). Tackling a growing cybersecurity threat in an increasingly connected industry. DNV. <https://www.dnv.com/expert-story/maritime-impact/tackling-a-growing-cybersecurity-threat-in-an-increasingly-connected-industry/>
- EMSA. (2022). CleanSeaNet service annual report 2022. European Maritime Safety Agency. <https://emsa.europa.eu>
- European Maritime Safety Agency. (2023). Common information sharing environment: Annual report. EMSA.
- Fernandez, J., Kim, S., & Liu, Y. (2023). Cybersecurity challenges in maritime transportation. *Applied Sciences*, 14(18), 8420. <https://doi.org/10.3390/app14188420>
- Howard, M., & Paret, P. (1984). On war (C. von Clausewitz). Princeton University Press.
- IFC. (2022). Annual report 2022. Information Fusion Centre, Singapore Navy.
- International Maritime Bureau. (2023). Piracy and armed robbery against ships: Annual report 2023. ICC.
- International Maritime Bureau. (2024). Piracy and armed robbery against ships: Annual report 2023. ICC. <https://www.icc-ccs.org>
- International Maritime Bureau. (2024). Piracy and armed robbery against ships: Annual report 2023. International Chamber of Commerce – IMB. https://www.icc-ccs.org/reports/2023_Annual_IMB_Piracy_and_Armed_Robbery_Report_live.pdf
- IOJI (Ocean Justice Initiative). (2024). Report of maritime detection & analysis in Indonesian waters. https://oceanjusticeinitiative.org/main/wp-content/uploads/2024/02/English-Version-of-Laporan-Deteksi-Marsec-IOJI_2023-2024-.pdf
- IOJI. (2024). Report of maritime detection & analysis in Indonesian waters. Indonesian Ocean Justice Initiative. <https://oceanjusticeinitiative.org>

- JICA. (2023). Maritime security technology cooperation in Asia. Japan International Cooperation Agency.
- Johnson, R. (2024, December 20). The strategic implications of AI on maritime security. RealClearDefense. <https://www.realcleardefense.com>
- Johnson, R. (2024, December 20). The strategic implications of AI on maritime security. RealClearDefense. <https://www.realcleardefense.com>
- KKP. (2024). Strategi pengendalian IUU fishing. Kementerian Kelautan dan Perikanan Republik Indonesia.
- Kroodsmas, D. A., Mayorga, J., Hochberg, T., Miller, N. A., Boerder, K., Ferretti, F., Wilson, A., Bergman, B., White, T. D., Block, B. A., Woods, P., Sullivan, B., Costello, C., & Worm, B. (2018). Tracking the global footprint of fisheries. *Science*, 359(6378), 904–908. <https://doi.org/10.1126/science.aao5646>
- Milne, R. (2025, June 18). Shadow fleets, cyber-attacks and spy ships: The crack security team braced for trouble at sea. *The Guardian*. <https://www.theguardian.com>
- Milne, R. (2025, June 18). Shadow fleets, cyber-attacks and spy ships: The crack security team braced for trouble at sea. *The Guardian*. <https://www.theguardian.com>
- Milne, R. (2025, June 18). Shadow fleets, cyber-attacks, and spy ships: The crack security team braced for trouble at sea. *The Guardian*. <https://www.theguardian.com>
- Moderndiplomacy. (2025). Illegal, unreported and unregulated fishing in the ASEAN region: Environmental and human security issues. <https://moderndiplomacy.eu/2025/01/14/illegal-unreported-and-unregulated-fishing-in-the-asean-region-environmental-and-human-security-issues/>
- Prakoso, L. Y. (2021). 01102021 Implementation Public Policy Model LYP [Dissertation summary]. ResearchGate. <https://doi.org/10.6084/m9.figshare.16725085.v1>
- Reuters. (2023, December 22). Ships rerouted by Red Sea crisis face overwhelmed African ports. <https://www.reuters.com/business/ships-rerouted-by-red-sea-crisis-face-overwhelmed-african-ports-2023-12-22/>
- Sherwood, H. (2025, May 4). The British engineer behind the US Navy's high-tech ocean drones. *The Times*. <https://www.thetimes.co.uk>
- Strobel, W. (2025, February 2). NATO steps up undersea infrastructure defense. *The Wall Street Journal*. <https://www.wsj.com>
- U.S. Coast Guard. (2024). Cyber trends and insights in the marine environment (CGCYBER 2024). U.S. Department of Homeland Security. <https://www.uscg.mil/Portals/0/Images/cyber/CGCYBER%202024%20CTIME.pdf>