

Adaptive Smart Defense Management: A Model for Integrating Land Power, Artificial Intelligence, Cyber Defense, and Autonomous Drone Systems to Strengthen Indonesia's Maritime Security

Fitry Taufiq Sahary1*

¹Kawasan IPSC Sentul, Jl. Anyar, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810

fitry.taufiq@idu.ac.id

*Corresponding Author

Article Info

Article history:

Received : 08 Juli, 2026

Revised : 08 Juli, 2026

Accepted : 08 Juli, 2026

Kata Kunci:

Artificial Intelligence;
Cyber Defense;
Drone;
Kekuatan Darat;
Keamanan Maritim;
Manajemen Pertahanan Modern.

ABSTRAK

Perkembangan ancaman keamanan maritim yang semakin kompleks menuntut transformasi manajemen pertahanan menuju sistem yang adaptif, terintegrasi, dan berbasis teknologi digital. Penelitian ini bertujuan merumuskan model *Adaptive Smart Defense Management* yang mengintegrasikan kekuatan darat, Artificial Intelligence (AI), *Cyber Defense*, *Big Data Analytics*, dan teknologi autonomous drone untuk meningkatkan efektivitas keamanan maritim Indonesia. Penelitian menggunakan pendekatan kualitatif dengan desain studi kasus dan *Soft Systems Methodology* (SSM) melalui wawancara, observasi, studi dokumentasi, dan analisis literatur. Hasil penelitian menunjukkan bahwa tantangan utama terletak pada belum optimalnya interoperabilitas sistem informasi, koordinasi antarlembaga, serta pemanfaatan teknologi digital dalam mendukung operasi multidomain. Model yang diusulkan mengintegrasikan fungsi manajemen modern dengan sistem pengambilan keputusan berbasis data, pengawasan realtime, dan kolaborasi lintas sektor. Implementasi model ini diharapkan mampu meningkatkan Maritime Domain Awareness, mempercepat respons terhadap ancaman multidomain, memperkuat ketahanan siber, serta mendukung terwujudnya sistem keamanan maritim Indonesia yang adaptif, efektif, dan berkelanjutan.

PENDAHULUAN

Perubahan lingkungan strategis global telah menggeser paradigma keamanan maritim dari pendekatan konvensional menuju sistem keamanan multidomain yang mengintegrasikan aspek darat, laut, udara, ruang siber, dan ruang informasi. Persaingan geopolitik di kawasan Indo-Pasifik, perkembangan teknologi digital, meningkatnya kejahatan lintas negara, serta penggunaan kecerdasan buatan (*Artificial Intelligence/AI*) dan sistem nirawak (*drone*) telah menciptakan spektrum ancaman baru yang jauh lebih kompleks dibandingkan dekade sebelumnya. Kondisi tersebut menuntut organisasi pertahanan untuk tidak hanya meningkatkan kapabilitas tempur, tetapi juga melakukan transformasi manajemen melalui penerapan Modern Defense Management yang adaptif, kolaboratif, dan berbasis teknologi digital (Prakoso, 2023; Teece, 2018; Bueger, 2015).

Keamanan maritim memiliki posisi yang sangat strategis karena sekitar 80% volume perdagangan internasional diangkut melalui jalur laut, sehingga gangguan terhadap keamanan laut akan berdampak langsung terhadap stabilitas ekonomi, logistik, energi,

dan ketahanan nasional suatu negara. Sebagai negara kepulauan terbesar di dunia, Indonesia memiliki lebih dari 17.000 pulau, wilayah laut sekitar 6,4 juta km², serta jalur pelayaran strategis yang menghubungkan Samudra Hindia dan Samudra Pasifik. Posisi geografis tersebut menjadikan Indonesia memiliki peluang ekonomi yang besar sekaligus menghadapi risiko keamanan yang tinggi akibat meningkatnya aktivitas kejahatan lintas negara dan rivalitas geopolitik di kawasan Indo-Pasifik.

Ancaman keamanan maritim saat ini berkembang dalam bentuk ancaman hibrida (*hybrid threats*). Ancaman tersebut meliputi *Illegal, Unreported and Unregulated Fishing* (IUU Fishing) penyelundupan narkoba, perdagangan manusia, pembajakan kapal, penyelundupan senjata, infiltrasi kelompok teroris melalui jalur laut, pencurian sumber daya alam, hingga serangan siber terhadap sistem pelabuhan, sistem navigasi, dan jaringan komando pertahanan. Menurut Prakoso dkk., ancaman nonmiliter telah menjadi tantangan dominan bagi keamanan maritim Indonesia sehingga memerlukan strategi penegakan hukum yang mengintegrasikan teknologi digital, koordinasi antarlembaga, serta modernisasi sistem pengawasan maritim.

Secara kuantitatif, peningkatan ancaman maritim dapat dilihat dari laporan ICC *International Maritime Bureau* (IMB) yang mencatat bahwa sepanjang tahun 2025 terjadi 137 insiden pembajakan dan perampokan bersenjata terhadap kapal, meningkat dibandingkan 116 insiden pada tahun 2024. Dari jumlah tersebut, 121 kapal berhasil dinaiki pelaku, 4 kapal dibajak, dan 42 insiden melibatkan penggunaan senjata api. Sebagian besar insiden terjadi di jalur pelayaran strategis Asia Tenggara, termasuk Selat Singapura yang berbatasan langsung dengan wilayah Indonesia. Kondisi ini menunjukkan bahwa kawasan maritim Indonesia tetap menjadi wilayah yang rentan terhadap gangguan keamanan regional.

Tabel 1. Perkembangan Ancaman Keamanan Maritim Global

Indikator	Nilai	Sumber
Perdagangan dunia melalui laut	±80%	UNCTAD Review of Maritime Transport 2024
Insiden pembajakan 2024	116 kasus	ICC IMB Annual Report 2025
Insiden pembajakan 2025	137 kasus	ICC IMB Annual Report 2025
Kapal berhasil dinaiki pelaku	121 kapal	ICC IMB Annual Report 2025
Penggunaan senjata api	42 kasus	ICC IMB Annual Report 2025

(Sumber: diolah penulis 2026)

Perkembangan ancaman tersebut tidak lagi hanya terjadi pada domain fisik, tetapi juga memasuki ruang digital. Digitalisasi pelabuhan, penerapan *Automatic Identification System* (AIS), *Electronic Chart Display Information System* (ECDIS), *Global Navigation Satellite System* (GNSS), dan sistem komando berbasis jaringan telah meningkatkan efisiensi operasional maritim. Namun, digitalisasi tersebut juga memperluas permukaan serangan (*attack surface*) yang dapat dimanfaatkan oleh aktor negara maupun non-negara melalui serangan siber, *GPS spoofing*, manipulasi AIS, *ransomware*, maupun gangguan terhadap sistem komunikasi pertahanan. Kajian mengenai keamanan siber maritim menunjukkan bahwa infrastruktur pelayaran modern semakin bergantung pada teknologi informasi sehingga membutuhkan tata kelola keamanan siber yang terintegrasi.

Disisi lain, perkembangan *Artificial Intelligence* (AI) telah membawa perubahan fundamental terhadap proses pengambilan keputusan strategis. AI memungkinkan organisasi pertahanan melakukan *predictive analytics*, identifikasi pola ancaman, deteksi dini aktivitas ilegal, serta pengambilan keputusan secara real-time melalui pemrosesan data satelit, radar, AIS, sensor pesisir, dan drone. Bersamaan dengan itu, teknologi **autonomous drone** memberikan kemampuan pengawasan wilayah laut yang lebih luas

dengan biaya operasional yang lebih efisien dibandingkan sistem patroli konvensional. Penelitian terbaru yang melibatkan Lukman Yudho Prakoso menegaskan bahwa integrasi ancaman siber dan drone merupakan tantangan utama keamanan maritim Indonesia pada masa depan sehingga membutuhkan transformasi strategi pertahanan nasional.

Dalam perspektif ilmu manajemen, perubahan lingkungan strategis tersebut menunjukkan bahwa pendekatan birokratis dan sektoral tidak lagi memadai. Organisasi pertahanan dituntut menerapkan *Modern Management* yang menekankan kemampuan organisasi untuk beradaptasi terhadap perubahan lingkungan melalui inovasi, kolaborasi, transformasi digital, serta pengambilan keputusan berbasis data. Konsep *Strategic Management* menempatkan proses perencanaan, pengorganisasian, pelaksanaan, dan pengendalian sebagai satu kesatuan yang harus didukung oleh informasi yang akurat, teknologi digital, dan sumber daya manusia yang kompeten. Sementara itu, teori *Dynamic Capability* menjelaskan bahwa organisasi yang mampu mengintegrasikan teknologi baru secara cepat akan memiliki keunggulan strategis dalam menghadapi perubahan lingkungan keamanan yang dinamis.

Dalam konteks keamanan maritim Indonesia, implementasi manajemen modern diwujudkan melalui integrasi berbagai pemangku kepentingan seperti TNI AD, TNI AL, Bakamla RI, Kementerian Perhubungan, Kepolisian, pemerintah daerah, serta masyarakat pesisir dalam satu ekosistem keamanan berbasis informasi. Menurut Prakoso, keberhasilan pengelolaan keamanan maritim tidak hanya ditentukan oleh kekuatan militer di laut, tetapi juga oleh kemampuan membangun sinergi antarlembaga, interoperabilitas teknologi, serta koordinasi kebijakan nasional. Oleh karena itu, keamanan maritim merupakan implementasi nyata dari *collaborative governance* dalam bidang pertahanan.

Kekuatan darat memiliki posisi strategis dalam sistem tersebut karena sebagian besar ancaman maritim berawal dari wilayah pesisir, pelabuhan, pulau-pulau kecil terluar, serta kawasan perbatasan. Aktivitas penyelundupan narkoba, perdagangan manusia, infiltrasi kelompok kriminal, hingga logistik kejahatan transnasional selalu memiliki keterkaitan dengan wilayah daratan. Oleh sebab itu, transformasi kekuatan darat menuju *Digital Land Power* menjadi kebutuhan strategis melalui pemanfaatan AI, drone, sensor cerdas, *command center*, serta sistem keamanan siber yang mampu mendukung operasi keamanan maritim secara terpadu. Integrasi tersebut sejalan dengan konsep *Multi-Domain Operations*, yaitu penyelenggaraan operasi pertahanan yang menghubungkan domain darat, laut, udara, siber, dan informasi dalam satu sistem komando yang adaptif.

Tabel 2. Transformasi Manajemen Modern dalam Keamanan Maritim

Dimensi Manajemen	Implementasi
Strategic Planning	Prediksi ancaman berbasis AI
Organizing	Integrasi TNI AD, TNI AL, Bakamla, Polri, K/L
Decision Support	Big Data Analytics dan AI
Coordinating	C4ISR dan Maritime Command Center
Controlling	Drone, satelit, AIS, dan Cyber Monitoring

(Sumber: diolah penulis (2026))

Meskipun transformasi digital telah berkembang pesat, implementasinya di Indonesia masih menghadapi berbagai kendala, antara lain belum optimalnya interoperabilitas sistem informasi antarlembaga, keterbatasan integrasi data pengawasan, belum adanya kerangka manajemen pertahanan digital yang menghubungkan kekuatan darat dengan keamanan maritim, serta belum optimalnya pemanfaatan AI dan drone dalam mendukung proses pengambilan keputusan strategis. Sebagian besar penelitian sebelumnya lebih menitikberatkan pada aspek operasi laut atau keamanan siber secara terpisah, sedangkan kajian yang mengintegrasikan *Modern Defense Management, Digital Land Power, Artificial Intelligence, Cyber Defense*, dan *Autonomous Drone* dalam satu model manajemen keamanan maritim masih sangat terbatas.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus yang dipadukan dengan pendekatan Soft Systems Methodology (SSM) untuk merancang model Modern Defense Management dalam mengintegrasikan kekuatan darat, Artificial Intelligence (AI), Cyber Defense, dan teknologi autonomous drone guna mendukung keamanan maritim Indonesia. Pendekatan kualitatif dipilih karena mampu mengeksplorasi secara mendalam dinamika organisasi, tata kelola, kolaborasi antarpemangku kepentingan, serta proses pengambilan keputusan dalam menghadapi ancaman keamanan maritim multidomain (Creswell & Poth, 2018). Sementara itu, SSM digunakan karena efektif untuk menganalisis permasalahan kompleks yang melibatkan banyak aktor, kepentingan, dan sistem yang saling berinteraksi, serta menghasilkan model konseptual yang aplikatif bagi pengambilan kebijakan (Checkland & Poulter, 2020).

Data penelitian diperoleh melalui wawancara mendalam dengan pemangku kepentingan di lingkungan TNI, Bakamla RI, Kementerian Pertahanan, dan instansi terkait, didukung observasi serta studi dokumentasi terhadap kebijakan, doktrin, dan literatur ilmiah. Analisis data dilakukan menggunakan model interaktif yang meliputi kondensasi data, penyajian data, dan penarikan kesimpulan secara iteratif untuk menghasilkan model manajemen yang valid dan implementatif (Miles, Huberman, & Saldaña, 2020). Validitas temuan diperkuat melalui triangulasi sumber, metode, dan teori sehingga model yang dihasilkan memiliki kredibilitas ilmiah serta relevansi praktis dalam mendukung transformasi digital keamanan maritim Indonesia (Yin, 2018).

HASIL DAN PEMBAHASAN

Kondisi Eksisting Manajemen Kekuatan Darat dalam Mendukung Keamanan Maritim Indonesia pada Era Digital

Transformasi lingkungan strategis global telah mengubah karakter ancaman keamanan maritim dari ancaman konvensional menjadi ancaman multidomain (multi-domain threats) yang melibatkan aspek fisik, siber, informasi, ekonomi, dan teknologi. Perkembangan tersebut dipengaruhi oleh meningkatnya digitalisasi sektor maritim,

kompetisi geopolitik di kawasan Indo-Pasifik, serta pemanfaatan Artificial Intelligence (AI), Internet of Things (IoT), Big Data Analytics, dan autonomous systems dalam operasi keamanan. Konsekuensinya, organisasi pertahanan tidak lagi cukup mengandalkan pendekatan sektoral berbasis domain tunggal, tetapi harus menerapkan Modern Defense Management yang mampu mengintegrasikan kekuatan darat, laut, udara, siber, dan ruang informasi secara terpadu (Bueger, 2015; Teece, 2018; Prakoso et al., 2024). Indonesia merupakan negara kepulauan dengan luas wilayah laut sekitar 6,4 juta km², garis pantai sekitar 108.000 km, serta lebih dari 17.000 pulau yang tersebar pada tiga Alur Laut Kepulauan Indonesia (ALKI). Kondisi geografis tersebut menjadikan Indonesia memiliki nilai strategis sekaligus kerentanan tinggi terhadap berbagai bentuk ancaman keamanan maritim.

Selain berfungsi sebagai jalur utama perdagangan internasional, wilayah perairan Indonesia juga menjadi lintasan kejahatan transnasional seperti penyelundupan narkoba, perdagangan manusia, Illegal, Unreported and Unregulated (IUU) Fishing, penyelundupan senjata, pembajakan kapal, hingga infiltrasi kelompok kriminal bersenjata (UNCTAD, 2024; Bueger, 2015). Menurut UNCTAD (2024), sekitar 80% volume perdagangan dunia diangkut melalui jalur laut. Besarnya ketergantungan terhadap transportasi laut menyebabkan gangguan keamanan maritim berdampak langsung terhadap stabilitas ekonomi global, rantai pasok, serta ketahanan energi. Sementara itu, International Maritime Bureau (IMB, 2025) melaporkan bahwa pada tahun 2025 terjadi 137 insiden pembajakan dan perampokan bersenjata terhadap kapal, meningkat dibandingkan 116 insiden pada tahun sebelumnya. Kawasan Asia Tenggara, khususnya Selat Singapura dan perairan sekitarnya, masih menjadi salah satu wilayah dengan tingkat kerawanan tertinggi.

Tabel 3. Indikator Strategis Keamanan Maritim Indonesia

Indikator	Nilai	Sumber
Luas wilayah laut Indonesia	±6,4 juta km ²	Kementerian Kelautan dan Perikanan (2023)
Garis pantai	±108.000 km	Badan Informasi Geospasial (2023)
Jumlah pulau	>17.000	Kementerian Dalam Negeri (2023)
Perdagangan dunia melalui laut	±80%	UNCTAD (2024)
Insiden pembajakan global 2025	137 kasus	IMB (2025)

(Sumber: diolah penulis (2026))

Data tersebut menunjukkan bahwa pengamanan wilayah maritim Indonesia tidak mungkin hanya mengandalkan unsur patroli laut. Sebagian besar aktivitas ilegal justru berawal dari wilayah daratan, seperti pelabuhan, kawasan pesisir, pusat logistik, dan pulau-pulau kecil terluar. Dengan demikian, kekuatan darat memiliki fungsi strategis sebagai lapisan pertama (first line of defense) dalam mendeteksi, mencegah, dan merespons ancaman sebelum berkembang menjadi gangguan di wilayah laut. Pandangan ini sejalan dengan hasil penelitian Prakoso et al. (2024) yang menekankan bahwa keamanan maritim memerlukan integrasi kekuatan darat dan laut melalui pendekatan kolaboratif berbasis teknologi digital.

Dalam perspektif ilmu manajemen, kondisi tersebut menunjukkan perlunya transformasi dari pola manajemen birokratis menuju Modern Defense Management. Manajemen modern tidak hanya berorientasi pada efisiensi organisasi, tetapi juga pada kemampuan organisasi membangun adaptabilitas, kolaborasi, inovasi, dan pengambilan keputusan berbasis data (Teece, 2018). Oleh karena itu, keberhasilan organisasi pertahanan tidak lagi ditentukan oleh besarnya sumber daya yang dimiliki, melainkan oleh kemampuan mengintegrasikan teknologi digital dengan proses manajerial secara efektif.

Penelitian Prakoso et al. (2024) mengenai pemanfaatan AI dalam ketahanan

keamanan maritim menunjukkan bahwa integrasi Artificial Intelligence mampu meningkatkan efektivitas *Maritime Domain Awareness* melalui analisis citra satelit, radar pantai, *Automatic Identification System* (AIS), dan sensor maritim secara real-time. AI memungkinkan organisasi melakukan prediksi pola ancaman, identifikasi kapal mencurigakan, serta pengambilan keputusan yang lebih cepat dibandingkan sistem konvensional. Temuan tersebut memperlihatkan bahwa teknologi bukan sekadar alat pendukung, melainkan telah menjadi bagian dari sistem manajemen organisasi pertahanan.

Selain AI, teknologi drone juga memberikan perubahan signifikan terhadap pola operasi keamanan maritim. Drone udara (*Unmanned Aerial Vehicle/UAV*) maupun drone permukaan (*Unmanned Surface Vehicle/USV*) mampu memperluas jangkauan pengawasan dengan biaya operasional yang lebih rendah dibandingkan patroli konvensional. Menurut Prakoso et al. (2025), penggunaan drone yang terintegrasi dengan AI mampu meningkatkan kecepatan deteksi aktivitas ilegal di wilayah pesisir dan laut, sekaligus mengurangi risiko personel dalam operasi pengamanan. Hal ini menunjukkan bahwa transformasi digital telah mengubah fungsi kekuatan darat dari sekadar penjaga wilayah menjadi pengelola sistem informasi keamanan maritim.

Di sisi lain, digitalisasi juga melahirkan ancaman baru berupa serangan siber terhadap infrastruktur maritim. Pelabuhan modern, sistem AIS, jaringan komunikasi, dan pusat komando pertahanan kini bergantung pada teknologi informasi yang rentan terhadap *malware*, *ransomware*, manipulasi data, hingga *GPS spoofing*. Ancaman tersebut berpotensi mengganggu operasi logistik nasional maupun operasi militer apabila tidak didukung oleh sistem Cyber Defense yang kuat (IMO, 2023). Oleh karena itu, kekuatan darat tidak hanya memerlukan kemampuan tempur konvensional, tetapi juga kompetensi dalam pengelolaan keamanan informasi dan perlindungan infrastruktur digital.

Dalam konteks organisasi, tantangan terbesar bukan terletak pada keterbatasan teknologi, melainkan pada interoperabilitas antarinstansi. Sistem informasi yang dimiliki TNI, Bakamla RI, Polri, Kementerian Perhubungan, dan kementerian/lembaga lainnya masih belum sepenuhnya terintegrasi sehingga pertukaran data sering kali berlangsung secara parsial. Akibatnya, proses deteksi dini dan respons terhadap ancaman menjadi kurang optimal. Menurut Prakoso et al. (2024), keberhasilan keamanan maritim Indonesia sangat dipengaruhi oleh kemampuan membangun kolaborasi lintas sektor, integrasi data, dan tata kelola informasi yang mendukung pengambilan keputusan secara cepat dan akurat.

Tabel 4. Analisis Kesenjangan Manajemen Kekuatan Darat dalam Mendukung Keamanan Maritim

Aspek	Kondisi Eksisting	Kondisi Ideal
Sistem informasi	Terpisah antarinstansi	Platform terpadu berbasis AI
Pengawasan	Patroli periodik	Pengawasan real-time berbasis sensor dan drone
Pengambilan keputusan	Reaktif	Prediktif berbasis AI
Koordinasi	Sektoral	Collaborative governance
Keamanan digital	Parsial	Cyber Defense terintegrasi
Operasi	Domain tunggal	Multi-Domain Operations

(Sumber: diolah penulis (2026))

Berdasarkan analisis tersebut, dapat disimpulkan bahwa kondisi eksisting manajemen kekuatan darat dalam mendukung keamanan maritim Indonesia masih menghadapi tantangan pada aspek integrasi organisasi, pemanfaatan teknologi digital,

interoperabilitas sistem informasi, dan tata kelola keamanan siber. Meskipun berbagai teknologi seperti AI, drone, dan *big data analytics* telah tersedia, implementasinya masih berjalan secara parsial dan belum menjadi bagian dari satu sistem manajemen pertahanan yang terpadu. Dengan demikian, menjawab rumusan masalah pertama, penelitian ini menemukan bahwa peningkatan efektivitas keamanan maritim memerlukan transformasi menuju *Modern Defense Management* yang mengintegrasikan *Land Power*, AI, *Cyber Defense*, dan teknologi nirawak dalam kerangka *Multi-Domain Operations*. Temuan ini menjadi dasar untuk merumuskan model konseptual yang akan dibahas pada bagian berikutnya mengenai desain *Adaptive Smart Defense Management Model* sebagai solusi manajerial bagi penguatan keamanan maritim Indonesia.

Perancangan *Adaptive Smart Defense Management Model* dalam Mendukung Keamanan Maritim Indonesia

Hasil analisis menunjukkan bahwa tantangan utama dalam pengelolaan keamanan maritim Indonesia tidak lagi hanya berkaitan dengan keterbatasan alutsista atau jumlah personel, tetapi juga menyangkut efektivitas sistem manajemen pertahanan dalam mengintegrasikan berbagai sumber daya, teknologi, dan pemangku kepentingan. Perubahan karakter ancaman yang semakin kompleks menuntut organisasi pertahanan mengembangkan sistem manajemen yang adaptif, responsif, dan berbasis teknologi digital. Dalam perspektif Strategic Management, organisasi yang mampu menyesuaikan strategi, struktur organisasi, dan pemanfaatan teknologi terhadap perubahan lingkungan akan memiliki keunggulan kompetitif yang lebih tinggi dibandingkan organisasi yang masih menggunakan pendekatan konvensional (David et al., 2020; Teece, 2018).

Konsep tersebut menjadi dasar dalam penyusunan *Adaptive Smart Defense Management Model*, yaitu model manajemen pertahanan modern yang mengintegrasikan kekuatan darat, *Artificial Intelligence (AI)*, *Cyber Defense*, *Big Data Analytics*, dan teknologi *autonomous drone* ke dalam satu sistem pengambilan keputusan yang terintegrasi. Model ini menempatkan fungsi manajemen—perencanaan (*planning*), pengorganisasian (*organizing*), pelaksanaan (*actuating*), dan pengendalian (*controlling*) sebagai fondasi utama dalam meningkatkan efektivitas operasi keamanan maritim. Pendekatan ini sejalan dengan hasil penelitian Prakoso et al. (2024), yang menegaskan bahwa transformasi digital pertahanan harus diawali dengan transformasi tata kelola organisasi agar pemanfaatan teknologi mampu memberikan nilai strategis terhadap peningkatan keamanan maritim.

Dalam implementasinya, kekuatan darat tidak lagi dipandang hanya sebagai unsur pertahanan teritorial, tetapi berkembang menjadi simpul integrasi informasi (*information hub*) yang menghubungkan data dari radar pantai, *Automatic Identification System (AIS)*, satelit, kamera pengawas, sensor maritim, hingga *Unmanned Aerial Vehicle (UAV)*. Integrasi data tersebut menghasilkan *Maritime Domain Awareness (MDA)* yang lebih komprehensif sehingga proses identifikasi ancaman dapat dilakukan secara lebih cepat, akurat, dan berkelanjutan. Menurut Bueger (2015), MDA merupakan fondasi utama dalam membangun sistem keamanan maritim modern karena memungkinkan organisasi memahami situasi operasional secara menyeluruh sebelum mengambil keputusan strategis.

Pemanfaatan *Artificial Intelligence* dalam model ini berfungsi sebagai *Decision Support System* yang mampu mengolah data dalam jumlah besar (*big data*) menjadi informasi yang relevan bagi pengambil keputusan. AI tidak hanya digunakan untuk mendeteksi aktivitas ilegal, tetapi juga melakukan analisis prediktif terhadap pola pergerakan kapal, potensi penyelundupan, maupun ancaman terhadap objek vital maritim. Temuan tersebut konsisten dengan penelitian Prakoso et al. (2024) yang

menyatakan bahwa penerapan AI pada sistem pengawasan maritim mampu meningkatkan kecepatan analisis informasi dan mendukung efektivitas operasi keamanan maritim berbasis data. Dengan demikian, pengambilan keputusan tidak lagi bersifat reaktif, melainkan berkembang menjadi *predictive decision making* yang didukung oleh analisis algoritma dan pembelajaran mesin (*machine learning*).

Komponen berikutnya adalah Cyber Defense, yang menjadi elemen penting dalam menjaga keberlangsungan sistem pertahanan digital. Digitalisasi infrastruktur maritim telah meningkatkan efisiensi pengelolaan pelabuhan, navigasi, dan komunikasi, namun di sisi lain memperbesar kerentanan terhadap serangan siber seperti *malware*, *ransomware*, manipulasi data AIS, maupun *Global Positioning System (GPS) spoofing*. Oleh karena itu, sistem keamanan siber harus menjadi bagian integral dari manajemen pertahanan modern untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi strategis (International Maritime Organization [IMO], 2023). Penelitian Prakoso et al. (2024) juga menekankan bahwa keberhasilan transformasi digital pertahanan sangat bergantung pada kemampuan organisasi dalam membangun ketahanan siber (*cyber resilience*) sebagai fondasi utama sistem keamanan nasional.

Selain AI dan keamanan siber, penggunaan autonomous drone memberikan nilai strategis sebagai *force multiplier* dalam operasi keamanan maritim. Drone mampu melaksanakan patroli secara berkelanjutan, menjangkau wilayah pesisir dan pulau-pulau kecil terluar, serta mengirimkan data visual secara *real time* ke pusat komando. Integrasi drone dengan AI memungkinkan proses identifikasi target berlangsung lebih cepat melalui teknologi *image recognition* dan *sensor fusion*. Dengan demikian, kebutuhan patroli konvensional dapat dikurangi tanpa mengurangi efektivitas pengawasan. Kondisi tersebut mendukung konsep Multi-Domain Operations, yaitu integrasi kemampuan darat, laut, udara, dan ruang siber dalam satu sistem operasi yang saling terhubung (Department of the Army, 2022).

Tabel 5. Komponen Adaptive Smart Defense Management Model

Komponen	Fungsi Strategis	Kontribusi terhadap Keamanan Maritim
Artificial Intelligence	Analisis prediktif dan <i>Decision Support System</i>	Mempercepat identifikasi ancaman
Big Data Analytics	Integrasi dan analisis data multisumber	Meningkatkan <i>Domain Awareness Maritime</i>
Cyber Defense	Perlindungan jaringan dan informasi	Menjamin sistem digital ketahanan
Autonomous Drone	Surveilans dan patroli otomatis	Memperluas pengawasan cakupan
Collaborative Command Center	Koordinasi lintas instansi	Mempercepat operasi respons

(Sumber: diolah penulis (2026))

Keberhasilan implementasi model tersebut sangat ditentukan oleh penerapan prinsip *collaborative governance*. Keamanan maritim merupakan tanggung jawab bersama yang melibatkan TNI, Bakamla RI, Kepolisian, kementerian teknis, pemerintah daerah, dan masyarakat pesisir. Oleh karena itu, interoperabilitas sistem informasi, standarisasi pertukaran data, serta sinkronisasi kebijakan menjadi prasyarat utama agar seluruh pemangku kepentingan dapat bekerja dalam satu kerangka operasi yang terpadu (Ansell & Gash, 2008). Sejalan dengan hal tersebut, Prakoso et al. (2024) menegaskan bahwa kolaborasi antarlembaga merupakan faktor penentu dalam membangun sistem keamanan maritim yang adaptif dan berkelanjutan.

Berdasarkan pembahasan tersebut, penelitian ini mengusulkan *Adaptive Smart Defense Management Model* sebagai pendekatan baru dalam pengelolaan keamanan

maritim Indonesia. Kebaruan model ini terletak pada integrasi antara fungsi-fungsi manajemen modern dengan teknologi AI, *Cyber Defense*, *Big Data Analytics*, dan *autonomous drone* dalam mendukung operasi keamanan maritim berbasis *Multi-Domain Operations*. Model ini tidak hanya memperkuat efektivitas pengawasan wilayah laut, tetapi juga meningkatkan kualitas pengambilan keputusan strategis, mempercepat koordinasi antarlembaga, serta memperkuat ketahanan maritim Indonesia dalam menghadapi ancaman multidomain pada era transformasi digital (Bueger, 2015; Prakoso et al., 2024; Teece, 2018).

KESIMPULAN

Penelitian ini menunjukkan bahwa penguatan keamanan maritim Indonesia tidak lagi dapat mengandalkan pendekatan konvensional yang berorientasi pada operasi sektoral, tetapi memerlukan transformasi menuju manajemen pertahanan modern yang adaptif, kolaboratif, dan berbasis teknologi digital. Integrasi kekuatan darat dengan *Artificial Intelligence* (AI), *Cyber Defense*, *Big Data Analytics*, dan teknologi drone mampu meningkatkan efektivitas pengawasan, mempercepat pengambilan keputusan, memperkuat koordinasi antarlembaga, serta mendukung pelaksanaan operasi multidomain dalam menghadapi ancaman keamanan maritim yang semakin kompleks. Model *Adaptive Smart Defense Management* yang diusulkan menjadi kerangka konseptual yang mengintegrasikan fungsi manajemen, teknologi, sumber daya manusia, dan tata kelola organisasi sehingga mampu meningkatkan ketahanan maritim nasional secara berkelanjutan.

Berdasarkan hasil penelitian, disarankan agar pemerintah mempercepat transformasi digital sektor pertahanan melalui pembangunan sistem informasi keamanan maritim yang terintegrasi, penguatan kemampuan keamanan siber, serta pemanfaatan AI dan drone sebagai bagian dari sistem pengawasan nasional. Sinergi antara TNI, Bakamla, Kepolisian, kementerian terkait, pemerintah daerah, perguruan tinggi, dan industri pertahanan perlu diperkuat melalui kebijakan yang mendukung interoperabilitas data, pengembangan sumber daya manusia digital, serta peningkatan riset dan inovasi teknologi pertahanan. Penelitian selanjutnya diharapkan dapat menguji model yang diusulkan secara empiris dengan menggunakan pendekatan kuantitatif atau metode campuran sehingga efektivitas implementasinya dapat diukur secara lebih komprehensif pada berbagai wilayah strategis maritim Indonesia.

DAFTAR PUSTAKA

- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571.
<https://doi.org/10.1093/jopart/mum032>
- Bueger, C. (2015). What is maritime security? *Marine Policy*, 53, 159–164.
<https://doi.org/10.1016/j.marpol.2014.12.005>
- Checkland, P., & Poulter, J. (2020). *Learning for action: A short definitive account of Soft Systems Methodology and its use for practitioners, teachers and students*. Wiley.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications.
- David, F. R., David, F. R., & David, M. E. (2020). *Strategic management: A competitive advantage approach, concepts and cases* (17th ed.). Pearson.
- Department of the Army. (2022). *Field Manual (FM) 3-0: Operations*. Headquarters, Department of the Army.
- International Maritime Bureau. (2025). *Piracy and armed robbery against ships: Annual report 2025*. ICC International Maritime Bureau.

- International Maritime Organization. (2021). *IMO cyber risk management*. International Maritime Organization.
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative data analysis: A methods sourcebook* (4th ed.). Sage Publications.
- Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. Free Press.
- Prakoso, L. Y. (2021). *Manajemen keamanan maritim*. Jakarta: Unhan Press.
- Prakoso, L. Y. (2022). *Strategi keamanan maritim Indonesia*. Jakarta: Unhan Press.
- Prakoso, L. Y., Risahdi, M., & Selamat, R. (2024). Artificial intelligence for maritime security resilience: Strengthening Indonesia's maritime defense through digital transformation. *Marco Polo: Journal of Maritime and Defense Studies*.
- Prakoso, L. Y., et al. (2024). Maritime security management based on artificial intelligence to support Indonesia's maritime resilience. *Journal of International Maritime Studies*.
- Prakoso, L. Y., et al. (2025). Artificial intelligence integration in maritime patrol operations to strengthen Indonesian maritime security. *Sosains: Jurnal Sosial dan Sains*.
- Prakoso, L. Y., et al. (2025). Cyber defense and autonomous drone integration for maritime security in Indonesia. *Journal of Indonesia Defense Studies*.
- Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, 51(1), 40–49. <https://doi.org/10.1016/j.lrp.2017.06.007>
- United Nations Conference on Trade and Development. (2024). *Review of maritime transport 2024*. United Nations.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.