

TRANSFORMASI KEAMANAN MARITIM ADAPTIF MELALUI INOVASI TEKNOLOGI KUANTUM DALAM MENGHADAPI ANCAMAN HIBRIDA GLOBAL

Dimas Gading

Universitas Pertahanan

dimasgadingap27@gmail.com

<http://doi.org/10.52307/jmi.v9i12.204>

Abstrak

Penelitian ini menganalisis pergeseran paradigma dalam keamanan maritim yang didorong oleh dua tren utama: meningkatnya ancaman hibrida dan kematangan teknologi kuantum. Analisis ini menunjukkan bahwa ancaman hibrida modern mengeksploitasi kerentanan fundamental, termasuk ambiguitas dalam deteksi, atribusi, dan hukum yang menciptakan kondisi "sea blindness," serta kerentanan siber pada infrastruktur digital dan navigasi yang semakin terintegrasi.

Temuan utama dari studi ini adalah bahwa teknologi kuantum menyediakan solusi simetris dan fundamental untuk kedua kerentanan tersebut. Sensor kuantum, termasuk PNT berbasis atom interferometer, magnetometri presisi berbasis NV-center, dan jaringan Distributed Quantum Sensing (DQS), menawarkan transparansi yang tinggi dan pengukuran akurat. Ini secara langsung mengurangi ambiguitas, mengatasi "sea blindness," dan mengubah kalkulasi strategis aktor hibrida dengan menghilangkan kemungkinan penyangkalan.

Selain itu, komunikasi kuantum, khususnya Underwater QKD (UQKD), memberikan keamanan absolut untuk tautan data kritis, yang memperkuat ketahanan Infrastruktur Maritim Kritis (CMI) dan arsitektur sensor terhadap intersepsi dan manipulasi siber. Sintesis dari sensor presisi, komunikasi aman, dan fusi data berbasis AI membentuk dasar bagi "arsitektur keamanan maritim adaptif" yang baru. Arsitektur ini bersifat proaktif, tahan banting, dan mampu beroperasi secara independen dari infrastruktur eksternal yang rentan.

Kata Kunci: Teknologi Kuantum, Ancaman hibrida modern, sea blindness, komunikasi kuantum

Abstract

This research analyzes the paradigm shift in maritime security driven by two main trends: the escalation of hybrid threats and the maturity of quantum technology. The analysis reveals that modern hybrid threats exploit fundamental vulnerabilities, including ambiguity in detection, attribution, and law, which creates conditions of "sea blindness," as well as cybersecurity vulnerabilities in increasingly integrated digital and navigational infrastructure.

The key finding of this study is that quantum technology offers symmetric and fundamental countermeasures to these vulnerabilities. Quantum sensors, including atom interferometer-based PNT, NV-center-based precision magnetometry, and Distributed Quantum Sensing (DQS) networks, provide high transparency and precise measurement. This directly

diminishes ambiguities, addresses "sea blindness," and alters the strategic calculus of hybrid actors by eliminating plausible deniability.

Additionally, quantum communication, particularly Underwater QKD (UQKD), offers absolute security for critical data links, enhancing the resilience of Critical Maritime Infrastructure (CMI) and sensor architecture against cyber interception and manipulation. The synthesis of precision sensors, secure communication, and AI-based data fusion forms the foundation for a new "adaptive maritime security architecture." This architecture is proactive, resilient, and capable of operating independently of vulnerable external infrastructure.

Keywords: Quantum Technology, Modern Hybrid Threats, Sea Blindness, Quantum Communication

A. PENDAHULUAN

Domain maritim telah lama menjadi fondasi utama bagi kemakmuran dan konektivitas global. Sebagai arteri vital perdagangan internasional, lautan memfasilitasi sekitar 90% volume perdagangan dunia (Lott, 2022) dan menopang konektivitas digital global, dengan 95% komunikasi data trans-regional melintasi kabel serat optik bawah laut (Bueger, 2023). Stabilitas di domain ini, oleh karena itu, bukan sekadar isu keamanan regional, melainkan prasyarat fundamental bagi stabilitas ekonomi dan politik global. Namun, lanskap ancaman yang dihadapi domain maritim telah mengalami evolusi signifikan. Paradigma keamanan maritim tradisional, yang berfokus pada konfrontasi angkatan laut simetris, kini ditantang oleh spektrum ancaman yang lebih kompleks, ambigu, dan asimetris (Lott, 2022).

Era kontemporer menyaksikan pergeseran menuju apa yang dikenal

sebagai "ancaman hibrida" (*hybrid threats*).

Ancaman ini didefinisikan sebagai tindakan koersif yang sengaja dirancang untuk tetap berada "di bawah ambang batas perang" (RAND Corporation, 2024). Aktor-aktor negara dan non-negara yang memanfaatkannya bertujuan untuk mencapai tujuan strategis baik itu keuntungan teritorial, disrupti ekonomi, maupun pelemahan tatanan internasional dengan mengeksploitasi ambiguitas, menghindari atribusi, dan memanipulasi "zona abu-abu" (*grey zones*) dalam hukum internasional (Lott, 2022).

Fokus utama dari ancaman hibrida maritim adalah Infrastruktur Maritim Kritis (CMI). Infrastruktur ini, yang mencakup kabel komunikasi bawah laut, pipa energi, ladang angin lepas pantai, dan pelabuhan, merupakan target bernilai tinggi (Mitrescu & Sokolov, 2025). Insiden sabotase terhadap pipa Nord Stream pada tahun 2022 dan kerusakan kabel Baltik telah berfungsi sebagai katalis yang mengejutkan,

menyoroti kerentanan ekstrem CMI. Perlindungan CMI secara inheren sulit; Bueger (2023) mengidentifikasi tantangan ini bersumber dari yurisdiksi yang kompleks (melintasi perairan teritorial, Zona Ekonomi Eksklusif, dan laut lepas), "materialitas lautan" (lingkungan yang keras dan sulit diawasi), serta sifat infrastruktur yang transnasional.

Kerentanan fisik ini diperburuk oleh fenomena kognitif yang diidentifikasi oleh Larsson (2024) sebagai "sea blindness" (kebutaan maritim). Konsep ini merujuk pada kegagalan kelembagaan dan kognitif di antara para pembuat kebijakan termasuk di institusi multilateral seperti PBB, NATO, dan Uni Eropa untuk sepenuhnya memahami, memprioritaskan, dan mempersiapkan diri menghadapi ancaman hibrida yang unik di domain maritim. Aktor hibrida berkembang pesat dalam bayang-bayang yang diciptakan oleh "sea blindness" ini.

Dimensi fundamental yang mengakselerasi ancaman hibrida maritim adalah domain siber. Transformasi digital yang cepat di sektor maritim melalui adopsi "smart ports," sistem navigasi terintegrasi, kapal otonom, dan *Internet of Things* (IoT) telah secara drastis memperluas "permukaan serangan siber" (Ben Farah, et al., 2022). Operasi siber bukan lagi sekadar pendukung, melainkan telah menjadi "strategi angkatan laut non-kinetik"

(Ferazza, 2025) dan merupakan komponen inti dari perang hibrida modern di laut.¹³ Serangan siber tidak hanya menargetkan data; mereka menargetkan sistem fisik (*cyber-physical systems*). Contohnya termasuk *GPS spoofing* untuk mengganggu navigasi kapal dan serangan *ransomware* yang melumpuhkan logistik pelabuhan vital, seperti yang dialami Maersk (Ben Farah, et al., 2022) dan pelabuhan lainnya (Clavijo Mesa, et al., 2024).

Di sinilah letak kesenjangan penelitian (*research gap*) utama yang coba dijawab oleh artikel ini. Di satu sisi, literatur keamanan maritim dan studi strategis (misalnya, Bueger, 2023; Lott, 2022; RAND Corporation, 2024; Ferazza, 2025) telah secara ekstensif mendefinisikan dan menganalisis *masalah* ancaman hibrida. Di sisi lain, literatur fisika terapan dan teknik (misalnya, Zwick, et al., 2023; Kim, et al., 2024; Aslam, et al., 2023) merinci kemajuan pesat dalam pengembangan *solusi* teknologi kuantum dalam mengatasi ancaman hibrida. Namun, hingga saat ini, terdapat kesenjangan konseptual dan analitis yang signifikan dalam menjembatani kedua domain diskursus ini. Analisis mengenai bagaimana kapabilitas spesifik teknologi kuantum yang sangat penting untuk di eskalasi dan dapat secara langsung mengatasi mekanisme fundamental yang dieksploitasi oleh

ancaman hibrida maritim masih sangat terbatas.

Artikel ini mengajukan tesis bahwa teknologi kuantum khususnya penginderaan presisi (*quantum sensing*) dan komunikasi aman (*quantum communication*) menawarkan sebuah pergeseran paradigma, bukan sekadar peningkatan inkremental, dalam keamanan maritim. Argumen intinya adalah bahwa teknologi kuantum secara fundamental meruntuhkan dua pilar utama yang menjadi sandaran strategi hibrida:

- 1) *Ambiguitas*, melalui kapabilitas pengukuran absolut dan *Maritime Domain Awareness* (MDA) presisi tinggi; dan
- 2) *Kerentanan Siber*, melalui jaminan keamanan tak bersyarat (*unconditional security*) yang didasarkan pada hukum fisika. Dengan demikian, teknologi kuantum memungkinkan terciptanya arsitektur keamanan maritim baru yang adaptif dan resilien.

B. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif-konseptual dengan desain deskriptif-analitis. Penelitian ini menggunakan pendekatan kualitatif-konseptual dengan desain deskriptif-analitis. Tujuannya adalah untuk membangun sebuah kerangka konseptual yang komprehensif mengenai penerapan

Arsitektur Teknologi Kuantum 2.0 dalam menangkal ancaman maritim hibrida dengan menganalisis, mensintesis, dan merekonstruksi temuan-temuan dari literatur yang telah ada.

Sifat penelitian ini didasarkan pada sintesis literatur interdisipliner yang mencakup bidang fisika kuantum, studi keamanan, kebijakan pertahanan, dan teknologi maritim. Metode pengumpulan data dilakukan melalui studi pustaka sistematis (*systematic literature review*) untuk mengidentifikasi, mengevaluasi, dan menginterpretasikan semua penelitian yang relevan dengan topik ini. Pendekatan ini dipilih karena dua alasan utama:

- 1) Sifat topik yang masih *emerging*, di mana teknologi kuantum yang relevan sebagian besar masih dalam tahap pengembangan dan uji laboratorium, sehingga data operasional primer di lapangan masih sangat terbatas; dan
- 2) Kesenjangan penelitian yang diidentifikasi berada pada level konseptual, yaitu kurangnya jembatan analitis antara literatur keamanan maritim (yang mendefinisikan masalah) dan literatur fisika terapan (yang mengembangkan solusi).

Metode inti yang digunakan adalah *Conceptual Framework Analysis*. Metode ini bertujuan untuk membangun jembatan analitis yang koheren antara dua atau lebih bidang studi yang sebelumnya terpisah.

Dalam konteks ini, penelitian berupaya membangun kerangka kerja baru "Arsitektur Keamanan Maritim Adaptif" dengan mengintegrasikan konsep-konsep dari studi keamanan (ancaman hibrida, zona abu-abu, CMI) dengan kapabilitas spesifik dari teknologi kuantum (sensor presisi, komunikasi aman).

Proses analisis dilakukan melalui tiga tahap yang sistematis:

1. Tahap 1: Dekonstruksi Ancaman. Tahap ini melibatkan dekonstruksi ancaman hibrida maritim, sebagaimana diidentifikasi dalam Tinjauan Pustaka (Bagian B.1). Fokusnya bukan hanya pada *taktik* (misalnya, sabotase), tetapi pada *mekanisme* atau *enabler* fundamental yang dieksploitasi oleh taktik tersebut. Analisis literatur (misalnya, Lott, 2022; RAND Corporation, 2024; Larsson, 2024; Ferazza, 2025) mengidentifikasi dua *enabler* utama:

- a) Ambiguitas, yang mencakup ambiguitas deteksi (kesulitan melihat apa yang terjadi di bawah air), ambiguitas atribusi (kesulitan membuktikan siapa pelakunya), dan ambiguitas hukum (memanfaatkan celah dalam UNCLOS) ; dan
- b) Kerentanan Siber, yaitu ketergantungan infrastruktur maritim modern pada sistem digital dan navigasi berbasis satelit yang rentan

terhadap intersepsi, manipulasi, dan disrupsi.

2. Tahap 2: Pemetaan Kapabilitas. Tahap ini mengidentifikasi dan memetakan kapabilitas teknologi kuantum spesifik yang relevan untuk mengatasi *enabler* pada Tahap 1, berdasarkan Tinjauan Pustaka (Bagian B.2). Kapabilitas yang dipetakan meliputi:

- a) PNT Kuantum (berbasis *atom interferometer*) untuk navigasi independent.
- b) Magnetometri presisi (berbasis *NV-center*) untuk deteksi anomali bawah air.
- c) *Distributed Quantum Sensing* (DQS) untuk pengawasan jaringan area luas dan
- d) *Underwater Quantum Key Distribution* (UQKD) untuk komunikasi aman.

3. Tahap 3: Sintesis Kerangka Kerja. Tahap akhir ini adalah sintesis, di mana kapabilitas yang dipetakan pada Tahap 2 secara sistematis diposisikan sebagai *counter-mechanism* (mekanisme penangkal) langsung terhadap kerentanan yang diidentifikasi pada Tahap 1. Proses pemetaan "masalah-ke-solusi" ini digunakan untuk membangun arsitektur keamanan maritim adaptif yang baru, yang disajikan secara rinci pada Bagian D.

C. PEMBAHASAN

Membangun Arsitektur Keamanan Maritim Adaptif Berbasis Kuantum

Analisis kerangka kerja konseptual menghasilkan temuan bahwa teknologi kuantum bukan sekadar menyediakan sensor atau saluran komunikasi yang lebih baik; ia berfungsi sebagai *enabler* fundamental bagi arsitektur keamanan yang secara kualitatif berbeda. Arsitektur ini dapat didefinisikan sebagai "adaptif"

karena ia mampu melakukan deteksi, fusi data, dan respons secara *real-time* (didorong oleh AI dan sensor kuantum), dan "resilien" karena ia mengurangi ketergantungan kritis pada sistem eksternal yang rentan (seperti GNSS) dan mengamankan integritas datanya melalui enkripsi kuantum.

Hubungan langsung antara vektor ancaman hibrida dan solusi kuantum yang mentransformasi dapat diringkas dalam kerangka kerja berikut:

Vektor Ancaman Hibrida	Kerentanan yang Dieksploitasi	Kapabilitas Kuantum (Solusi)
Perang Elektronik (GPS Spoofing/Jamming)	Ketergantungan total pada sinyal GNSS eksternal (GPS, Galileo, BeiDou)	Navigasi Inersia Kuantum (PNT Kuantum berbasis Atom Interferometer)
Sabotase Infrastruktur Kritis Bawah Laut (CMI)	"Sea Blindness"; Opasitas laut; Kesulitan pengawasan area luas	Jaringan Sensor Kuantum Terdistribusi (DQS) untuk pengawasan CMI
Infiltrasi Aset Siluman (UUV, Kapal Selam Kecil)	Ambiguitas deteksi (Akustik rendah); Kesulitan atribusi	Magnetometri Presisi (<i>Magnetic Anomaly Detection</i> / MAD berbasis NV-center)
Penyadapan Komunikasi C2 & Data Sensor	Kerentanan enkripsi klasik (terhadap intersepsi & <i>quantum computing</i>)	Komunikasi Kuantum Aman (<i>Underwater Quantum Key Distribution</i> / UQKD)

Tabel 1: Kerangka Transformasi Keamanan Maritim: Memetakan Solusi Kuantum terhadap Vektor Ancaman Hibrida

Temuan 1: Revolusi Maritime Domain Awareness (MDA) melalui Penginderaan Kuantum

Temuan pertama adalah bahwa penginderaan kuantum secara fundamental mengubah paradigma

Maritime Domain Awareness (MDA) dengan menggantikan deteksi probabilistik dengan pengukuran absolut, sehingga secara langsung mengikis "ambiguitas" yang menjadi sandaran ancaman hibrida.

Menghilangkan Ambiguitas (1): Navigasi Presisi dalam Lingkungan GNSS-Denied

Ancaman hibrida maritim sering memanifestasikan dirinya sebagai perang elektronik, di mana sinyal *Global Navigation Satellite System* (GNSS) di-*jamming* (diganggu) atau, yang lebih berbahaya, di-*spoofing* (dipalsukan) (Ben Farah, et al., 2022). Serangan ini mengeksploitasi ketergantungan mutlak navigasi modern pada sinyal eksternal.

Teknologi kuantum menawarkan solusi definitif melalui *Positioning, Navigation, and Timing* (PNT) berbasis kuantum. Sensor inersia kuantum, seperti *atom interferometers*, berfungsi sebagai *inertial measurement units* (IMU) yang mampu mengukur percepatan dan rotasi dengan presisi yang ribuan kali lebih baik daripada sistem klasik (SPIE Proceedings, 2024). Karena sensor ini bersifat *self-contained* (internal) dan tidak bergantung pada sinyal eksternal apa pun, mereka kebal terhadap *jamming* dan *spoofing* GNSS.

Implikasi strategisnya sangat besar: kapal angkatan laut, dan akhirnya kapal

komersial kritis, yang dilengkapi dengan PNT kuantum dapat mempertahankan akurasi navigasi absolut bahkan di tengah serangan siber atau elektronik yang intens. Ini bukan lagi fiksi ilmiah; ini adalah "fokus awal" dari program pertahanan praktis seperti AUKUS Pillar II (CSIS, 2023), yang bertujuan memberikan resiliensi navigasi kepada aset-aset di Indo-Pasifik.

Menghilangkan Ambiguitas (2): Mendeteksi yang Tidak Terdeteksi (Deteksi Bawah Laut)

Pilar kedua dari ambiguitas hibrida adalah opasitas (kekeruhan) domain bawah laut. Aktor hibrida dapat menggunakan *Unmanned Underwater Vehicles* (UUV) siluman atau kapal selam kecil untuk melakukan sabotase CMI atau infiltrasi teritorial dengan probabilitas deteksi yang rendah.

Sensor kuantum berbasis *NV-center* menawarkan kapabilitas *Magnetic Anomaly Detection* (MAD) generasi baru. Beroperasi pada suhu kamar, sensor ini memiliki sensitivitas ekstrem untuk mendeteksi "gangguan terkecil" dalam medan magnet bumi yang disebabkan oleh benda logam feromagnetik, seperti lambung kapal selam atau UUV.

Namun, penting untuk memberikan nuansa kritis pada kapabilitas ini. Sebuah tesis MIT (2025) yang menganalisis dampak strategis magnetometri kuantum

berargumen bahwa teknologi ini *tidak* akan "membuat lautan menjadi transparan". Alasannya terletak pada fisika dasar: anomali magnetik dari sebuah objek menurun sebanding dengan *pangkat tiga terbalik* dari jarak. Ini berarti, bahkan peningkatan sensitivitas sensor sepuluh kali lipat hanya menghasilkan peningkatan jangkauan deteksi sekitar dua kali lipat. Oleh karena itu, tesis tersebut menyimpulkan bahwa dampaknya untuk *Peperangan Anti-Kapal Selam (ASW) strategis* yaitu, melacak kapal selam rudal balistik (SSBN) di lautan terbuka yang luas akan terbatas.

Meskipun analisis Tesis MIT tersebut valid untuk ASW strategis, ia tidak sepenuhnya relevan untuk skenario *ancaman hibrida*. Ancaman hibrida bukanlah SSBN yang berpatroli di Atlantik Utara, melainkan UUV yang mengancam *titik CMI tertentu* (misalnya, pipa Baltik) atau kapal selam kecil yang beroperasi di *selat sempit*. Dalam skenario pengawasan area lokal dan terbatas ini, keterbatasan jangkauan sensor tunggal dapat diatasi dengan *jaringan sensor*. Di sinilah konsep *Distributed Quantum Sensing (DQS)* (Kim, et al., 2024) menjadi sangat relevan. Solusinya bukanlah satu sensor super yang mahal, melainkan jaringan sensor NV-center yang lebih kecil dan terdistribusi, yang dihubungkan secara kuantum untuk mengawasi aset CMI bernilai tinggi.

Arsitektur MDA: Integrasi Jaringan Sensor Kuantum (DQS) dengan AI

Arsitektur keamanan adaptif yang baru muncul dari sintesis jaringan sensor kuantum (DQS) dengan pemrosesan data berbasis *Artificial Intelligence (AI)*. Saat ini, arsitektur sensor canggih telah menunjukkan kelayakan integrasi ini. Studi oleh Karst, et al. (2025) mendemonstrasikan penggunaan *pelampung akustik* yang ditenagai AI untuk deteksi dan pelacakan kapal secara *real-time*. Dalam sistem ini, AI berfungsi sebagai otak fusi data di *edge*, memungkinkan MDA yang persisten.

Kerangka kerja yang diusulkan di sini adalah mengganti atau melengkapi *input* data akustik (yang rentan terhadap kebisingan dan kondisi lingkungan) dengan *input* data kuantum fidelitas tinggi dari jaringan DQS berbasis NV-center. Jaringan sensor kuantum ini akan menyediakan data mentah yang jauh lebih presisi ke *AI-driven fusion engine*, seperti yang diulas oleh Miller (2025) dalam konteks deteksi ancaman siber maritim. Integrasi *DQS + AI* ini menciptakan sistem MDA persisten yang secara proaktif memantau CMI, mengubah "sea blindness" (Larsson, 2024) menjadi transparansi domain yang komprehensif.

Temuan 2: Memperkuat Resiliensi Infrastruktur (CMI) melalui Komunikasi Kuantum

Arsitektur sensor canggih pada Temuan 1 menciptakan data dalam jumlah besar. Namun, arsitektur ini hanya sekuat tautan komunikasi yang mentransmisikan data tersebut. Vektor ancaman hibrida kedua, kerentanan siber, secara khusus menargetkan komunikasi *Command-and-Control* (C2) dan data sensor itu sendiri (Ferazza, 2025).

Mengamankan Komunikasi C2 dan Data Sensor

Quantum Key Distribution (QKD) menyediakan solusi definitif untuk mengamankan data *backhaul* ini.⁴³ Dengan menggunakan QKD untuk mengamankan tautan antara aset maritim (pelampung sensor, kapal patroli, UUV pengumpul data) dan stasiun komando di darat, integritas dan kerahasiaan data sensor dapat dijamin dengan keamanan tak bersyarat. Ini berarti data MDA yang dihasilkan oleh sensor kuantum tidak dapat disadap atau dimanipulasi tanpa terdeteksi.

Aplikasi Niche untuk Underwater QKD (UQKD)

Di sinilah *Underwater QKD* (UQKD) menemukan *niche* strategisnya yang unik. Seperti yang dibahas dalam Tinjauan Pustaka, UQKD masih dalam tahap awal dan sangat terbatas dalam jangkauan

(mungkin hanya ratusan meter). Oleh karena itu, ia tidak akan menggantikan komunikasi satelit (SATCOM) untuk C2 jarak jauh.

Namun, UQKD sangat ideal untuk mengamankan *tautan jarak pendek* yang paling rentan dan kritis dalam arsitektur perlindungan CMI. Contoh skenario meliputi:

1. Mengamankan tautan komunikasi antara *sensor DQS di dasar laut* dengan *UUV otonom* yang datang untuk mengumpulkan data secara berkala.
2. Mengamankan tautan antara UUV tersebut dengan *pelampung permukaan* yang kemudian akan mentransmisikan data ke satelit (setelah dienkripsi dengan kunci QKD).
3. Mengamankan komunikasi antar-sensor dalam jaringan pelindung CMI yang padat.

Dalam arsitektur ini, UQKD (Tutorial, 2023) berfungsi sebagai *perisai* (shield) kriptografis untuk *pedang* (sword) sensor kuantum. Ini secara langsung menangkal ancaman siber-fisik (Ferazza, 2025) pada level infrastruktur fisik itu sendiri.

Implikasi Strategis dan Tantangan

Sintesis dari temuan-temuan ini menunjukkan adanya pergeseran fundamental dalam kalkulus strategis keamanan maritim. Esensi dari operasi

zona abu-abu (RAND Corporation, 2024) dan manuver hukum hibrida (Lott, 2022) adalah *plausible deniability* (penyangkalan yang masuk akal). Aktor hibrida beroperasi dalam ambiguitas, mengandalkan fakta bahwa tindakan mereka sulit dideteksi dan lebih sulit lagi untuk diatribusikan secara pasti.

Arsitektur keamanan maritim adaptif berbasis kuantum menghancurkan pilar *deniability* tersebut. Sensor PNT kuantum dan jaringan DQS tidak memberikan data probabilistik; mereka memberikan *transparansi* dan *atribusi* berbasis pengukuran fisika yang absolut. Ketika sebuah UUV tak dikenal terdeteksi mendekati kabel bawah laut secara *real-time* oleh jaringan sensor magnetik, ambiguitas hilang. Aktor hibrida kehilangan ruang manuvernya; ia dipaksa untuk memilih antara membatalkan operasi atau mengambil risiko eskalasi terbuka.

Tentu saja, tantangan adopsi sangat besar. Realisme menuntut pengakuan akan hambatan dalam hal kesiapan teknologi, biaya, dan tuntutan lingkungan operasional laut yang keras (tekanan tinggi, salinitas, suhu) (Crawford, 2021). Transisi dari prototipe laboratorium ke sistem yang tangguh di lapangan akan membutuhkan investasi besar dan rekayasa yang inovatif.

Bagi negara maritim seperti Indonesia, implikasinya sangat mendalam.

Dengan *roadmap* teknologi kuantum yang sedang disusun oleh BRIN, Indonesia memiliki peluang strategis. Daripada mencoba bersaing secara langsung di semua lini (seperti komputasi kuantum skala besar), Indonesia dapat memfokuskan investasinya pada *niche* strategis yang memiliki dampak asimetris tertinggi terhadap keamanan nasionalnya:

- 1) pengembangan sensor PNT kuantum untuk mencapai kedaulatan dan resiliensi navigasi bagi armada militer dan komersialnya, dan
- 2) pengembangan jaringan sensor magnetik terdistribusi untuk pengawasan CMI di jalur pelayaran dan *chokepoints* kritis.

D. PENUTUP

Penelitian ini menganalisis pergeseran paradigma dalam keamanan maritim yang didorong oleh konvergensi dua tren: eskalasi ancaman hibrida dan kematangan teknologi kuantum. Analisis ini menegaskan bahwa ancaman hibrida maritim modern beroperasi dengan mengeksploitasi dua kerentanan fundamental:

- 1) *Ambiguitas* dalam deteksi, atribusi, dan hukum yang menciptakan kondisi "sea blindness" dan

2) *Kerentanan siber* pada infrastruktur digital dan navigasi yang semakin terintegrasi.

Temuan utama dari penelitian ini adalah bahwa teknologi kuantum menawarkan mekanisme penangkal (*counter-mechanism*) yang simetris dan fundamental terhadap kedua kerentanan tersebut. Pertama, sensor kuantum termasuk PNT berbasis *atom interferometer*, magnetometri presisi berbasis *NV-center*, dan jaringan *Distributed Quantum Sensing* (DQS) menghadirkan tingkat *transparansi absolut* dan pengukuran presisi. Ini secara langsung mengikis ambiguitas, mengatasi "sea blindness," dan mengubah kalkulus strategis aktor hibrida dengan menghilangkan *plausible deniability*. Kedua, komunikasi kuantum terutama *Underwater QKD* (UQKD) menawarkan *keamanan absolut* untuk tautan data kritis, memperkuat resiliensi CMI dan arsitektur sensor terhadap intersepsi dan manipulasi siber.

Sintesis dari sensor presisi, komunikasi aman, dan fusi data berbasis AI ini membentuk fondasi bagi "arsitektur keamanan maritim adaptif" yang baru. Arsitektur ini bersifat proaktif, resilien, dan mampu beroperasi secara independen dari infrastruktur eksternal yang rentan.

Berdasarkan temuan ini, dirumuskan beberapa rekomendasi:

1. Bagi negara-negara maritim, terutama Indonesia dengan inisiatif *Quantum Readiness* dari BRIN (2024), disarankan untuk memprioritaskan R&D dan adopsi teknologi kuantum ke dalam *roadmap* pertahanan dan keamanan nasional.
2. Investasi harus difokuskan pada *niche* strategis dengan dampak asimetris tertinggi, daripada mencoba bersaing di setiap domain kuantum. Dua prioritas utama yang diidentifikasi adalah:
 - a) Penguasaan sensor PNT kuantum untuk mencapai independensi dan resiliensi navigasi, dan
 - b) Pengembangan jaringan sensor magnetik terdistribusi (DQS) untuk pengawasan CMI di *chokepoints* dan perairan kritis.

E. DAFTAR PUSTAKA

Buku dan Report

- Lanzagorta, M. (2011). Quantum radar. Morgan & Claypool Publishers.
- Lott, A. (2022). The Implications of Hybrid Threats to the Maritime Domain. Leiden: Brill.
- RAND Corporation. (2024). Understanding and Countering China's Maritime Gray Zone Operations. Santa Monica, CA: RAND Corporation.

SPIE Proceedings. (2024). Quantum Technologies for Defence and Security 2024. Bellingham, WA: SPIE.

The NATO Maritime Unmanned Systems Initiative. (2020). Emerging and disruptive technologies in the maritime domain: Implications for NATO. NATO ACT.

UNIDIR. (2024). Quantum Technology, Peace and Security: A Primer. Geneva, Switzerland: UNIDIR.

U.S. Department of Defense. (2021). Quantum science and technology strategy. Diambil dari <https://www.defense.gov>

Jurnal Ilmiah

Aslam, N., Zhou, H., Urbach, E. K., Turner, M. J., Walsworth, R. L., Lukin, M. D., & Park, H. (2023). Quantum sensors for biomedical applications. *Nature Reviews Physics*, 5(3), 157–169.

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, 13(1), 22.

Bueger, C. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy*, 155, 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. *Information*, 15(11), 710.

Crawford, S. E., Shugayev, R. A., Paudel, H. P., Lu, P., Syamlal, M., Ohodnicki, P. R.,... Gentry, R. (2021). Quantum

sensing for energy applications: Review and perspective. *Advanced Quantum Technologies*, 4(8), 2100049.

Degen, C. L., Reinhard, F., & Cappellaro, P. (2017). Quantum sensing. *Reviews of Modern Physics*, 89(3), 035002. <https://doi.org/10.1103/RevModPhys.89.035002>

Dowling, J. P., & Milburn, G. J. (2003). Quantum technology: The second quantum revolution. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 361(1809), 1655–1674. <https://doi.org/10.1098/rsta.2003.1227>

Ferazza, F. (2025). The role of cyber operations in modern maritime conflict. *Cybersecurity*, 11(1).

Geng, M., et al. (2025). Advances of Quantum Key Distribution and Network Nonlocality. *Entropy*, 27(9), 950.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, 74(1), 145–195. <https://doi.org/10.1103/RevModPhys.74.145>

Gyongyosi, L., & Imre, S. (2019). A survey on quantum computing technology. *Computer Science Review*, 31, 51–71. <https://doi.org/10.1016/j.cosrev.2018.11.002>

Karst, J., McGurrin, R., Gavin, K., Luttrell, J., Rippey, W., Coniglione, R.,... Riedel, R. (2025). Enhancing

- Maritime Domain Awareness Through AI-Enabled Acoustic Buoys for Real-Time Detection and Tracking of Fast-Moving Vessels. *Sensors*, 25(6), 1930.
- Kim, D. H., Hong, S., Kim, Y. S., Kim, Y., Lee, S. W., Pooser, R. C.,... Lim, H. T. (2024). Distributed quantum sensing of multiple phases with fewer photons. *Nature Communications*, 15(1), 266.
- Larsson, O. L. (2024). Sea blindness in grey zone preparations. *Defence Studies*, 24(3), 399–420.
- Martínez, F., Sánchez, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2024). Maritime cybersecurity: protecting digital seas. *International Journal of Information Security*, 23(2), 1429–1457.
- Miller, T. (2025). Artificial Intelligence in Maritime Cybersecurity: A Systematic Review of AI-Driven Threat Detection and Risk Mitigation Strategies. *Electronics/MDPI*.
- Mitrescu, S., & Sokolov, M. (2025). Hybrid Threats and the Challenge to Maritime Infrastructure. Dalam *Science for Peace & Security series*. Springer.
- Montenegro, V., Mukhopadhyay, C., Yousefjani, R., Sarkar, S., Mishra, U., Paris, M. G. A., & Bayat, A. (2025). Review: Quantum metrology and sensing with many-body systems. *Physics Reports*, 1134, 1–62.
- Peng, P., Xie, X., Claramunt, C., Lu, F., Gong, F., & Yan, R. (2025). Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. *Transportation Research Part E: Logistics and Transportation Review*, 195(C).
- Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2, 79. <https://doi.org/10.22331/q-2018-08-06-79>
- Shah, V., & Wakai, R. T. (2022). A practical guide to optical magnetometry with atomic vapors. *Journal of Applied Physics*, 131(21), 210901. <https://doi.org/10.1063/5.0088532>
- Stensrud, C. J., & Østhagen, A. (2024). Hybrid Warfare at Sea? Russia, Svalbard and the Arctic. *Scandinavian Journal of Military Studies*, 7(1), 111–130.
- Zwick, A. E., & Álvarez, G. A. (2023). Quantum sensing tools to characterize physical, chemical and biological processes with magnetic resonance. *Journal of Magnetic Resonance Open*, 16–17, 100113.

Website

- A tutorial on Underwater Quantum Key Distribution. (2023). IEEE Xplore / ArXiv.
- Gover, A. (2022). Quantum technology in the maritime domain: A primer. The Royal Institution for Naval Research. Diambil dari <https://www.rinr.org.uk>