JURNAL CINTA NUSANTARA

Volume 04 Nomor 022023
E-ISSN: 3025-4469
https://jurnalbundaratu.org/journal/index.php/cintanusantarajournal

Strategi Pengembangan Giant Sea Wall Jakarta sebagai Infrastruktur Pertahanan Maritim Strategis Guna Memperkuat Keamanan Wilayah Ibu Kota

Sunu Tri Yuana[1]*, Bagus Jatmiko[2] , Elisabeth Tanti[3]

[1,2,3] Sekolah Staf dan Komando Angkatan Laut, Jakarta, Indonesia
**Corresponding author: sunutriyuana47@gmail.com*

Abstrak

Giant Sea Wall Jakarta selama ini terutama diperdebatkan sebagai instrumen pengendalian banjir pesisir dan adaptasi terhadap kenaikan muka air laut. Perspektif tersebut penting, tetapi belum sepenuhnya menjelaskan nilai strategis infrastruktur pesisir ketika berada pada kawasan yang menopang pelabuhan, logistik, energi, komunikasi, transportasi, pelayanan publik, dan fungsi pemerintahan. Artikel ini bertujuan merumuskan strategi pengembangan Giant Sea Wall Jakarta sebagai infrastruktur sipil strategis yang mendukung pertahanan maritim tanpa mengarah pada militerisasi proyek. Penelitian menggunakan pendekatan kualitatif melalui tinjauan literatur naratif-konseptual yang menyintesis kajian mengenai sekuritisasi pertahanan pesisir, maritime critical infrastructure protection, ketahanan infrastruktur, keamanan fisik dari ancaman asimetris, multi-agency command and control, dan keamanan siber maritim. Hasil analisis menunjukkan bahwa nilai pertahanan Giant Sea Wall tidak semata terletak pada kemampuannya menahan ancaman hidrometeorologis, melainkan pada potensinya menjadi bagian dari arsitektur perlindungan berlapis yang menjaga kontinuitas fungsi strategis, mendukung kesadaran situasional maritim, memperkuat koordinasi lintas lembaga, dan meningkatkan ketahanan sistem kendali digital. Artikel ini mengembangkan Integrated Maritime Defense Infrastructure Framework (IMDIF) yang direvisi ke dalam lima lapisan: spektrum ancaman, perlindungan fisik dan operasional, kontinuitas fungsi kritis, integrasi komando-kendali dan informasi, serta resiliensi siber dan kelembagaan. Kerangka tersebut menempatkan Giant Sea Wall sebagai dual-use strategic infrastructure yang fungsi utamanya tetap sipil, namun desain, tata kelola, dan kesiapsiagaannya dapat memberikan nilai tambah bagi pertahanan maritim dan keamanan wilayah Jakarta.

Kata Kunci: Giant Sea Wall Jakarta; pertahanan maritim; infrastruktur maritim kritis; sekuritisasi; command and control; keamanan siber.

Abstract

The Jakarta Giant Sea Wall has primarily been debated as an instrument for coastal flood control and adaptation to sea-level rise. While this perspective remains important, it does not fully capture the strategic value of coastal infrastructure situated within an area that supports ports, logistics, energy, communications, transportation, public services, and governmental functions. This article aims to formulate a strategy for developing the Jakarta Giant Sea Wall as strategic civil infrastructure that supports maritime defense without leading to the militarization of the project. The study employs a qualitative approach through a narrative-conceptual literature review, synthesizing scholarship on the securitization of coastal defense, maritime critical infrastructure protection, infrastructure resilience, physical security against asymmetric threats, multi-agency command and control, and maritime cybersecurity. The analysis demonstrates that the defense value of the Giant Sea Wall lies not merely in its capacity to withstand hydrometeorological hazards, but also in its potential to become part of a layered protection architecture that safeguards the continuity of strategic functions, supports maritime situational awareness, strengthens inter-agency coordination, and enhances the resilience of digital control systems. This article develops a revised Integrated Maritime Defense Infrastructure Framework (IMDIF) consisting of five layers: the threat spectrum; physical and operational protection; continuity of critical functions; command, control, and information integration; and cyber and institutional resilience. The framework conceptualizes the Giant Sea Wall as dual-use strategic infrastructure whose primary function remains civilian, while its design, governance, and preparedness can provide additional value for maritime defense and the security of the Jakarta metropolitan area.

Keywords: *Jakarta Giant Sea Wall; maritime defense; maritime critical infrastructure; securitization; command and control; cybersecurity.*

1. PENDAHULUAN

Kawasan pesisir Jakarta menghadapi tekanan yang tidak hanya berdimensi lingkungan, tetapi juga berdimensi strategis. Banjir pesisir, penurunan muka tanah, gangguan sistem drainase, dan kenaikan muka air laut dapat memengaruhi kawasan dengan konsentrasi tinggi penduduk, kegiatan ekonomi, pelabuhan, jaringan logistik, energi, telekomunikasi, transportasi, dan layanan publik. Karena itu, gangguan di pesisir Jakarta tidak berhenti pada kerusakan fisik akibat genangan, tetapi dapat berkembang menjadi gangguan berantai terhadap fungsi yang menopang mobilitas, distribusi barang, pelayanan negara, dan aktivitas ekonomi. Kajian mengenai Jakarta menunjukkan bahwa penurunan muka tanah dan kenaikan muka laut tetap menjadi faktor penting yang memperbesar risiko pesisir, sehingga perlindungan wilayah membutuhkan infrastruktur yang andal dan tata kelola jangka panjang (Takagi et al., 2017; Garschagen et al., 2018).

Dalam konteks tersebut, Giant Sea Wall muncul sebagai salah satu instrumen perlindungan pesisir yang dapat dipandang melampaui fungsi konvensional pengendalian banjir. Perubahan sudut pandang diperlukan karena infrastruktur pesisir berskala besar berada di ruang yang sama dengan aktivitas maritim strategis. Pelabuhan dan jaringan pendukungnya, misalnya, memiliki nilai ekonomi sekaligus nilai pertahanan karena gangguan terhadapnya dapat menurunkan kemampuan negara mempertahankan aliran logistik dan mengoperasikan fungsi penting. Watts (2005) menunjukkan bahwa infrastruktur maritim kritis menjadi strategis karena keterhubungannya dengan perdagangan, mobilitas nasional, dan proyeksi kekuatan; gangguan pada pelabuhan dapat menghasilkan konsekuensi ekonomi, keamanan, dan operasional yang jauh lebih besar daripada kerusakan fisik awal.

Perkembangan ancaman juga memperluas alasan untuk melihat infrastruktur pesisir melalui perspektif pertahanan. Ancaman terhadap infrastruktur maritim kontemporer tidak hanya berasal dari bencana alam atau konflik konvensional, tetapi juga dari sabotase, terorisme, serangan menggunakan wahana kecil, gangguan terhadap fasilitas vital, dan serangan siber terhadap sistem operasi. Kiciński et al. (2019) memperlihatkan bahwa fasilitas maritim dan kapal yang berada di pelabuhan memerlukan perlindungan fisik khusus terhadap ancaman asimetris dari arah perairan. Giraud et al. (2011) menunjukkan perkembangan sistem pengamanan infrastruktur offshore yang menggabungkan sensor, deteksi perilaku mencurigakan, analisis situasi, dan respons bertingkat. Pada saat yang sama, digitalisasi sektor maritim meningkatkan ketergantungan pada AIS, VTS, SCADA, jaringan komunikasi, sensor, dan sistem kendali, sehingga gangguan siber dapat berubah menjadi gangguan keselamatan dan kontinuitas operasi (Cichocki & Wójcik, 2025).

Literatur mengenai Giant Sea Wall Jakarta masih lebih banyak berfokus pada hidrologi, adaptasi perubahan iklim, reklamasi, penurunan muka tanah, dan dampak sosial-ekologis. Sementara itu, literatur pertahanan pesisir di Indonesia mulai menunjukkan bahwa ancaman lingkungan dapat ditempatkan dalam agenda keamanan ketika berpotensi mengganggu keselamatan masyarakat dan fungsi negara. Lievonne et al. (2025), melalui kajian Delta Works, memperlihatkan bahwa pertahanan pesisir dapat dipahami melalui proses sekuritisasi dan bahwa keberhasilannya ditopang oleh komitmen jangka panjang, transparansi, dan keterlibatan masyarakat. Namun, kajian tersebut belum secara khusus mengintegrasikan pertahanan fisik terhadap ancaman asimetris, perlindungan infrastruktur maritim kritis, komando-kendali lintas lembaga, dan resiliensi siber ke dalam pembahasan Giant Sea Wall Jakarta.

Kesenjangan tersebut menjadi dasar artikel ini. Persoalannya bukan apakah Giant Sea

Wall harus diubah menjadi instalasi militer, melainkan bagaimana infrastruktur sipil strategis dapat dirancang dan dikelola agar mendukung pertahanan maritim. Dalam artikel ini, fungsi pertahanan dipahami sebagai kemampuan infrastruktur untuk membantu menjaga wilayah pesisir, mempertahankan kontinuitas aset dan layanan strategis, menyediakan dukungan bagi pemantauan dan respons, serta meningkatkan ketahanan terhadap spektrum ancaman alamiah maupun buatan manusia. Posisi ini menjaga batas konseptual yang jelas: Giant Sea Wall tetap merupakan infrastruktur sipil, tetapi dapat memiliki nilai dual-use ketika standar keandalan, sistem pengamanan, konektivitas data, prosedur darurat, dan tata kelolanya mempertimbangkan kebutuhan keamanan nasional.

Berdasarkan argumentasi tersebut, penelitian ini menjawab pertanyaan: bagaimana Giant Sea Wall Jakarta dapat dikembangkan sebagai infrastruktur sipil strategis yang mendukung pertahanan maritim dan keamanan wilayah Jakarta? Tujuannya adalah merumuskan strategi pengembangan dan membangun kerangka konseptual yang menghubungkan sekuritisasi pertahanan pesisir, maritime critical infrastructure protection, perlindungan fisik, kontinuitas fungsi strategis, multi-agency command and control, serta resiliensi siber. Kebaruan artikel terletak pada pengembangan ulang Integrated Maritime Defense Infrastructure Framework (IMDIF) yang tidak lagi menempatkan adaptasi pesisir sebagai poros tunggal, melainkan menjadikan ketahanan infrastruktur maritim strategis sebagai pusat analisis.

2. METODE

Penelitian ini menggunakan pendekatan kualitatif melalui tinjauan literatur naratif-konseptual. Pendekatan dipilih karena tujuan penelitian adalah membangun sintesis teoretis dan kebijakan mengenai posisi Giant Sea Wall Jakarta sebagai infrastruktur strategis pendukung pertahanan maritim, bukan mengukur pengaruh antarvariabel atau mengestimasi efektivitas teknis konstruksi.

Literatur dikelompokkan ke dalam lima klaster. Klaster pertama mencakup Giant Sea Wall, NCICD, banjir pesisir Jakarta, dan penurunan muka tanah untuk memberikan konteks ancaman. Klaster kedua mencakup sekuritisasi dan coastal defense, terutama pembelajaran dari Delta Works. Klaster ketiga mencakup maritime critical infrastructure protection, ketahanan infrastruktur, dan kontinuitas layanan. Klaster keempat membahas perlindungan fisik terhadap ancaman asimetris, sistem pengawasan, dan graded response. Klaster kelima mencakup keamanan siber pada sistem transportasi dan infrastruktur maritim.

Pemilihan sumber didasarkan pada relevansi langsung terhadap fungsi strategis infrastruktur, keterhubungan dengan ruang maritim, dan kemampuan sumber menjelaskan mekanisme perlindungan atau tata kelola. Artikel mengenai Giant Sea Wall yang hanya berfokus pada aspek desain hidrologis atau perdebatan adaptasi tidak dijadikan pusat analisis, tetapi digunakan secara terbatas untuk menjelaskan latar ancaman dan kebutuhan keandalan sistem. Sebaliknya, kajian mengenai MCIP, komando-kendali lintas lembaga, pengamanan fisik fasilitas maritim, dan keamanan siber diprioritaskan untuk mengembangkan orientasi pertahanan.

Analisis dilakukan dalam tiga tahap. Pertama, identifikasi spektrum ancaman dan fungsi strategis yang perlu dipertahankan. Kedua, pemetaan prinsip perlindungan fisik, operasional, digital, dan kelembagaan dari setiap klaster literatur. Ketiga, sintesis antarprinsip untuk membentuk IMDIF yang direvisi. Karena kerangka yang dihasilkan bersifat konseptual, penelitian ini tidak mengklaim bahwa setiap fitur pengamanan dapat langsung diterapkan pada desain Giant Sea Wall tanpa kajian teknis, hukum, lingkungan, dan operasional lebih lanjut.

3. TINJAUAN PUSTAKA DAN KERANGKA TEORETIS

Sekuritisasi dan Pertahanan Pesisir

Teori sekuritisasi menjelaskan bagaimana suatu isu yang semula dipandang sebagai persoalan kebijakan biasa dapat dinaikkan menjadi isu keamanan ketika dipresentasikan sebagai ancaman serius terhadap objek rujukan tertentu, seperti negara, masyarakat, wilayah, atau fungsi vital. Dalam kerangka Copenhagen School, sekuritisasi tidak hanya bergantung pada karakter ancaman, tetapi juga pada proses politik dan penerimaan audiens terhadap kebutuhan tindakan yang lebih terkoordinasi dan mendesak (Buzan et al., 1998). Perspektif ini relevan untuk pertahanan pesisir karena ancaman banjir, kenaikan muka laut, dan kegagalan infrastruktur dapat berubah dari persoalan teknis menjadi persoalan keamanan apabila konsekuensinya mengancam keselamatan publik dan kontinuitas fungsi negara.

Kajian Lievonne et al. (2025) mengenai Delta Works memperlihatkan bagaimana perlindungan pesisir dapat diletakkan dalam kerangka pertahanan melalui komitmen negara, pembangunan kelembagaan, partisipasi masyarakat, transparansi, dan keberlanjutan program. Pelajaran penting dari pengalaman Belanda bukan semata skala konstruksinya, tetapi pembentukan institusi dan legitimasi jangka panjang untuk mempertahankan sistem perlindungan. Bagi Jakarta, sekuritisasi tidak seharusnya diartikan sebagai pemindahan kewenangan sipil kepada militer. Sebaliknya, sekuritisasi berfungsi sebagai dasar untuk mengakui bahwa kegagalan perlindungan pesisir dapat memiliki konsekuensi strategis sehingga membutuhkan perencanaan lintas sektor, standardisasi keandalan, dan kesiapsiagaan yang lebih tinggi.

Maritime Critical Infrastructure Protection

Maritime Critical Infrastructure Protection (MCIP) berangkat dari pemahaman bahwa pelabuhan, fasilitas energi, sistem navigasi, jalur logistik, terminal, dan jaringan pendukung maritim memiliki fungsi yang sangat penting bagi ekonomi dan keamanan. Watts (2005) menegaskan bahwa karakter pelabuhan modern yang terbuka, padat aktivitas, dan bergantung pada jaringan teknis membuatnya sekaligus penting dan rentan. Serangan atau gangguan pada satu bagian dapat menghasilkan efek ekonomi, operasional, dan psikologis yang lebih luas, termasuk gangguan terhadap distribusi dan kemampuan mobilisasi.

MCIP juga menekankan bahwa perlindungan aset maritim tidak cukup dilakukan oleh satu organisasi. Watts (2005) mengembangkan argumen mengenai multi-agency command and control melalui fusion center yang menyatukan informasi, pengawasan, perencanaan, serta tindakan berbagai lembaga. Prinsip yang paling relevan bagi Giant Sea Wall adalah adanya common operating picture, pertukaran data, koordinasi lintas kewenangan, dan perencanaan skenario secara bersama. Dengan demikian, infrastruktur fisik tidak berdiri sendiri, tetapi menjadi bagian dari sistem keamanan yang menghubungkan sensor, operator, penegak hukum, pertahanan, pengelola pelabuhan, pemerintah daerah, dan lembaga teknis.

Ketahanan Infrastruktur Strategis dan Kontinuitas Fungsi

Infrastruktur strategis memperoleh nilai kritis dari layanan yang dipertahankannya, bukan hanya dari ukuran fisiknya. Little (2002) menunjukkan bahwa sistem infrastruktur yang saling terhubung memiliki potensi cascading failure ketika kegagalan satu layanan memicu gangguan pada layanan lain. Dalam sistem pesisir yang bergantung pada pompa, listrik, telekomunikasi, sensor, pintu air, jaringan jalan, pelabuhan, dan pusat kendali, ketergantungan semacam ini menjadi sangat penting. Karena itu, resiliensi menuntut

redundansi, kapasitas pemulihan, prosedur kontinjensi, dan kemampuan mempertahankan fungsi minimum ketika sebagian komponen gagal.

Ninkovic (2021) menempatkan ketahanan infrastruktur kritis sebagai kemampuan untuk mengantisipasi, menyerap, beradaptasi, dan pulih dari gangguan. Prinsip tersebut mengubah orientasi dari sekadar "melindungi struktur" menjadi "mempertahankan fungsi". Dalam konteks Giant Sea Wall, indikator keberhasilan strategis tidak hanya berupa integritas tanggul, melainkan juga kontinuitas pelabuhan, akses logistik, layanan energi dan komunikasi, mobilitas darurat, serta kemampuan operator untuk menjalankan sistem dalam kondisi krisis.

Perlindungan Fisik, Surveillance, dan Graded Response

Ancaman asimetris dari arah perairan menuntut lapisan pengamanan yang berbeda dari pertahanan konvensional. Kiciński et al. (2019) menunjukkan bahwa penghalang terapung dapat digunakan sebagai elemen perlindungan fasilitas maritim dari ancaman wahana kecil berkecepatan tinggi. Temuan tersebut tidak berarti bahwa struktur Giant Sea Wall dapat secara langsung disamakan dengan barrier anti-serangan, tetapi memperlihatkan prinsip penting bahwa perlindungan waterside membutuhkan desain fisik, zona aman, dan perangkat penghalang khusus yang disesuaikan dengan aset yang dilindungi.

Giraud et al. (2011) melalui sistem SARGOS memperluas prinsip tersebut dari perlindungan pasif menuju perlindungan aktif berbasis informasi. Sistem yang mereka kaji mengintegrasikan radar, sensor lain, klasifikasi target, deteksi perilaku mencurigakan, penilaian tingkat bahaya, dan respons bertingkat dengan validasi operator. Secara konseptual, model ini relevan bagi pengembangan Giant Sea Wall karena menunjukkan bahwa infrastruktur strategis modern perlu menggabungkan hard protection dengan situational awareness dan decision support. Dengan demikian, nilai pertahanan tidak hanya melekat pada beton atau tanggul, tetapi pada kemampuan sistem mendeteksi anomali, memahami situasi, berkomunikasi, dan merespons secara proporsional.

Keamanan Siber Infrastruktur Maritim

Digitalisasi menjadikan keamanan siber bagian dari keamanan fisik infrastruktur. Cichocki dan Wójcik (2025) mengidentifikasi ketergantungan sektor maritim pada GNSS, AIS, VTS, ECDIS, SCADA, IoT, serta sistem komunikasi dan logistik. Keterhubungan tersebut meningkatkan efisiensi, tetapi sekaligus memperluas attack surface dan memungkinkan serangan siber mengganggu operasi pelabuhan, navigasi, komunikasi, pengendalian proses, dan rantai pasok.

Implikasinya bagi Giant Sea Wall sangat langsung. Infrastruktur pesisir berskala besar yang menggunakan sensor tinggi muka air, sistem pompa otomatis, pintu air, kamera, jaringan komunikasi, pusat kendali, dan SCADA tidak boleh diperlakukan sebagai struktur sipil yang terpisah dari keamanan siber. Resiliensi harus mencakup segmentasi jaringan, kontrol akses, pemantauan anomali, cadangan komunikasi, prosedur manual, pembaruan sistem, latihan insiden, dan koordinasi respons siber. Dengan demikian, perlindungan fisik dan digital perlu dipandang sebagai satu kesatuan.

4. HASIL DAN PEMBAHASAN

Reposisi Giant Sea Wall sebagai Infrastruktur Sipil Strategis Pendukung Pertahanan Maritim

Pengembangan Giant Sea Wall perlu direposisi dari diskursus yang hanya menempatkannya sebagai tanggul pengendali banjir menuju diskursus infrastruktur strategis. Reposisi ini tidak mengurangi fungsi dasar perlindungan pesisir. Justru, fungsi perlindungan menjadi titik awal untuk menilai konsekuensi yang lebih luas: kawasan apa yang dilindungi, layanan apa yang dipertahankan, dan bagaimana gangguan pada kawasan tersebut memengaruhi keamanan wilayah. Ketika suatu infrastruktur membantu menjaga pelabuhan, jalur distribusi, jaringan energi, komunikasi, transportasi, dan fasilitas negara, maka nilai strategisnya berasal dari fungsi yang dipertahankan.

Konsep ini sejalan dengan MCIP. Watts (2005) menempatkan pelabuhan sebagai node yang menghubungkan perdagangan dan kekuatan nasional, sehingga kerusakan pada infrastruktur maritim memiliki konsekuensi yang tidak proporsional terhadap kerusakan awal. Bagi Jakarta, Giant Sea Wall dapat dipahami sebagai protective infrastructure yang memperkecil peluang gangguan fisik pada kawasan pesisir sekaligus menyediakan ruang untuk membangun lapisan pengamanan tambahan. Namun, label "pertahanan maritim" harus digunakan secara disiplin. Giant Sea Wall bukan alat tempur, tidak menggantikan patroli, dan bukan basis militer. Ia merupakan infrastruktur sipil dengan fungsi dual-use: melindungi masyarakat dan ekonomi dalam kondisi normal serta mendukung kontinuitas fungsi strategis dalam kondisi krisis.

Reposisi tersebut juga memperkuat alasan mengapa keandalan proyek harus dinilai dengan standar yang lebih tinggi. Infrastruktur dengan implikasi strategis harus memiliki toleransi terhadap kegagalan, redundansi sistem kritis, rencana operasi darurat, dan mekanisme pemulihan. Status strategis tidak boleh berhenti sebagai label administratif, tetapi harus menghasilkan konsekuensi pada desain, operasi, pemeliharaan, keamanan, dan latihan kesiapsiagaan.

Tabel 1. Reposisi Fungsi Giant Sea Wall dalam Perspektif Pertahanan Maritim

Dimensi	Pendekatan konvensional	Pendekatan strategis pertahanan maritim
Fungsi utama	Pengendalian banjir pesisir	Perlindungan pesisir sekaligus kontinuitas fungsi strategis
Objek yang dilindungi	Kawasan daratan dan permukiman	Masyarakat, pelabuhan, logistik, energi, komunikasi, transportasi, dan layanan publik
Keamanan	Keselamatan struktur	Perlindungan berlapis, waterside security, surveillance, kesiapsiagaan, dan respons
Operasi	Pompa, pintu air, dan pemeliharaan	Operasi normal, continuity plan, cadangan sistem, latihan, dan pemulihan

Dimensi	Pendekatan konvensional	Pendekatan strategis pertahanan maritim
Digital	Otomasi dan monitoring teknis	Cyber resilience, kontrol akses, segmentasi, pemantauan anomali, dan prosedur manual
Tata kelola	Koordinasi proyek	Multi-agency command and control, data fusion, dan akuntabilitas lintas lembaga

Spektrum Ancaman dan Konsep Perlindungan Berlapis

Orientasi pertahanan memerlukan perluasan spektrum ancaman. Ancaman pertama tetap berupa gangguan alam dan hidrometeorologis yang dapat menurunkan fungsi kawasan pesisir. Namun, infrastruktur strategis juga harus mempertimbangkan ancaman buatan manusia, seperti sabotase, intrusi dari arah perairan, terorisme, vandalisme terhadap komponen kritis, serangan terhadap fasilitas energi atau komunikasi, serta tindakan yang sengaja ditujukan untuk menghentikan operasi. Spektrum ketiga berasal dari kegagalan teknologi dan siber, termasuk manipulasi sensor, gangguan komunikasi, kompromi sistem kendali, atau serangan terhadap jaringan yang menghubungkan pompa, pintu air, pusat kendali, dan layanan pelabuhan.

Karena ancamannya beragam, satu lapisan perlindungan tidak memadai. Giant Sea Wall perlu dilihat sebagai bagian dari layered defense yang memadukan physical protection, surveillance, access management, redundancy, emergency response, dan cyber resilience. Literatur Kiciński et al. (2019) penting pada tingkat prinsip karena memperlihatkan bahwa ancaman wahana kecil di perairan membutuhkan physical stand-off dan barrier khusus untuk menjaga fasilitas strategis. Penerapannya pada Giant Sea Wall tidak berarti memasang satu jenis barrier di seluruh struktur, melainkan melakukan penilaian risiko terhadap titik yang berdekatan dengan fasilitas vital, pusat kendali, intake, pintu air, terminal, atau area dengan konsekuensi tinggi apabila disusupi.

Lapisan kedua adalah surveillance dan deteksi anomali. SARGOS menunjukkan pendekatan yang menggabungkan beberapa sensor untuk mendeteksi, mengklasifikasikan, dan menilai perilaku target sebelum operator menentukan respons (Giraud et al., 2011). Prinsip tersebut dapat diterapkan secara konseptual melalui maritime domain awareness yang terintegrasi dengan pengelolaan Giant Sea Wall. Sistem radar, kamera, AIS, sensor perimeter, dan informasi dari otoritas pelabuhan tidak perlu berdiri sebagai sistem terpisah. Data dapat difusikan pada pusat kendali untuk membentuk common operating picture yang membantu operator membedakan aktivitas normal, kondisi keselamatan, dan anomali keamanan.

Lapisan ketiga adalah graded response. Respons terhadap gangguan tidak boleh bersifat tunggal dan otomatis. Dalam model SARGOS, tingkat respons disesuaikan dengan karakter ancaman dan divalidasi operator. Bagi Giant Sea Wall, prinsip ini berarti tersedianya protokol mulai dari verifikasi alarm, pembatasan akses, peringatan, aktivasi unsur pengamanan, koordinasi dengan otoritas pelabuhan dan penegak hukum, sampai aktivasi prosedur darurat. Pendekatan bertingkat mengurangi risiko overreaction sekaligus mempercepat tindakan pada insiden yang benar-benar berbahaya.

Lapisan keempat adalah continuity protection. Skenario keamanan tidak hanya bertanya apakah tanggul rusak, tetapi apakah sistem tetap dapat menjalankan fungsi minimum. Jika

listrik utama terganggu, apakah pompa dan pusat kendali memiliki cadangan? Jika komunikasi digital terputus, apakah tersedia saluran alternatif? Jika satu akses logistik tertutup, apakah ada jalur pengganti? Perspektif ini menggeser fokus dari protection of assets menuju protection of functions, sesuai dengan prinsip ketahanan infrastruktur kritis (Little, 2002; Ninkovic, 2021).

Kontinuitas Infrastruktur Maritim Kritis dan Efek Berantai

Nilai strategis Giant Sea Wall terutama muncul ketika analisis diarahkan pada interdependensi. Pelabuhan tidak dapat berfungsi hanya karena dermaga tetap kering. Operasinya membutuhkan akses jalan, listrik, sistem digital, pergudangan, bahan bakar, tenaga kerja, keamanan, komunikasi, dan hubungan dengan jaringan hinterland. Demikian pula sistem pompa dan pintu air membutuhkan listrik, komunikasi, sensor, operator, suku cadang, serta akses perbaikan. Kegagalan salah satu node dapat memicu gangguan pada node lain.

Dalam kerangka pertahanan maritim, kontinuitas layanan harus ditetapkan sebagai outcome utama. Ini berarti pemerintah perlu mengidentifikasi critical functions yang harus dipertahankan dalam berbagai skenario. Pelabuhan, distribusi bahan bakar, komunikasi darurat, akses ke fasilitas publik, jalur mobilisasi, dan pelayanan dasar dapat memiliki prioritas yang berbeda. Penetapan prioritas memungkinkan investasi diarahkan pada redundansi, cadangan energi, pemisahan jalur, stockpile komponen tertentu, serta prosedur recovery yang jelas.

Pendekatan tersebut juga memperkuat logika dual-use. Infrastruktur yang memiliki cadangan energi, komunikasi alternatif, pusat kendali yang aman, dan jalur operasi darurat akan lebih tangguh menghadapi banjir maupun gangguan buatan manusia. Dengan demikian, peningkatan nilai pertahanan tidak selalu membutuhkan komponen militer. Banyak kapasitas yang relevan bagi pertahanan justru berupa peningkatan reliability dan resilience sistem sipil.

Multi-Agency Command and Control sebagai Inti Tata Kelola Operasional

Tantangan utama Giant Sea Wall bukan hanya fragmentasi kewenangan administratif, tetapi juga kebutuhan koordinasi operasional ketika insiden terjadi. Collaborative governance penting untuk menyelaraskan perencanaan, namun pada kondisi krisis diperlukan struktur komando, aliran informasi, dan pembagian tugas yang lebih tegas. Watts (2005) menunjukkan bahwa perlindungan infrastruktur maritim memerlukan command and control lintas lembaga yang mampu mengintegrasikan intelijen, sensor, fungsi regulasi, penegakan hukum, dan kekuatan respons dalam satu gambaran situasi.

Pelajaran yang dapat diadaptasi bukan menyalin kelembagaan Amerika Serikat, melainkan mengadopsi prinsip fusion. Giant Sea Wall membutuhkan mekanisme yang menyatukan operator teknis, pemerintah daerah, pengelola pelabuhan, lembaga hidrometeorologi, unsur keamanan, penegak hukum, layanan darurat, operator energi dan telekomunikasi, serta institusi pertahanan sesuai kebutuhan. Dalam kondisi normal, mekanisme tersebut berfungsi untuk pertukaran data, latihan, dan pemeliharaan kesiapsiagaan. Dalam kondisi darurat, ia harus mampu menghasilkan common operating picture, menetapkan prioritas, dan mengoordinasikan respons secara cepat.

Multi-agency command and control juga menjawab masalah bahwa keamanan fisik, keselamatan, dan keamanan siber sering dikelola oleh unit berbeda. Insiden modern dapat bersifat hybrid. Gangguan sensor dapat didahului oleh intrusi siber, sementara serangan fisik dapat disertai disinformasi atau gangguan komunikasi. Karena itu, pemisahan absolut antara

keamanan teknis dan keamanan operasional akan memperlambat deteksi dan respons. Integrasi informasi menjadi unsur yang lebih penting daripada sekadar penambahan jumlah perangkat pengamanan.

Resiliensi Siber sebagai Komponen Pertahanan Giant Sea Wall

Sistem Giant Sea Wall yang semakin otomatis akan memperbesar ketergantungan terhadap teknologi digital. Cichocki dan Wójcik (2025) menunjukkan bahwa sektor maritim modern menggunakan sistem yang saling terhubung dan menghadapi ancaman seperti ransomware, phishing, spoofing, DDoS, kompromi kredensial, dan serangan terhadap SCADA. Pada konteks Giant Sea Wall, risiko utama bukan hanya kehilangan data, tetapi hilangnya kemampuan melihat kondisi lapangan, mengendalikan pompa atau pintu air, mengoordinasikan respons, dan menjaga kontinuitas operasi.

Karena itu, cybersecurity by design harus menjadi bagian dari desain strategis, bukan tambahan setelah sistem beroperasi. Pertama, jaringan teknologi operasional perlu dipisahkan secara proporsional dari jaringan administratif. Kedua, akses harus mengikuti prinsip least privilege dan autentikasi yang kuat. Ketiga, sistem kritis membutuhkan logging, deteksi anomali, pembaruan, dan mekanisme pemulihan. Keempat, harus tersedia prosedur manual atau mode degradasi apabila otomasi gagal. Kelima, latihan insiden harus menggabungkan skenario fisik dan siber agar organisasi tidak memperlakukan keduanya sebagai domain yang terpisah.

Aspek siber juga memperkuat kebutuhan multi-agency command and control. Operator Giant Sea Wall mungkin memiliki kompetensi teknis, tetapi penanganan serangan siber dapat memerlukan dukungan lembaga khusus, operator telekomunikasi, pengelola pelabuhan, dan aparat keamanan. Karena itu, protokol berbagi informasi dan eskalasi insiden perlu dirancang sebelum krisis terjadi.

Pembelajaran Delta Works dan Legitimasi Pertahanan Pesisir

Penguatan orientasi pertahanan tidak dapat mengabaikan legitimasi sosial. Lievonne et al. (2025) menunjukkan bahwa Delta Works berkembang melalui komitmen jangka panjang, institusi khusus, pembiayaan berkelanjutan, transparansi, dan keterlibatan masyarakat. Pelajaran tersebut penting karena infrastruktur pertahanan pesisir memiliki umur yang panjang dan membutuhkan pemeliharaan lintas pemerintahan. Tanpa legitimasi dan kepastian kelembagaan, fungsi strategis yang direncanakan pada tahap awal dapat melemah karena perubahan anggaran, prioritas, atau pembagian kewenangan.

Sekuritisasi karena itu harus dibedakan dari militarisasi. Menempatkan risiko pesisir sebagai isu keamanan berarti meningkatkan prioritas koordinasi dan kesiapsiagaan, bukan mengurangi transparansi atau partisipasi. Justru, semakin strategis sebuah infrastruktur, semakin tinggi tuntutan akuntabilitasnya. Pemerintah perlu menjelaskan fungsi yang dilindungi, standar keandalan, tanggung jawab operator, mekanisme pemeliharaan, dan batas keterlibatan sektor pertahanan. Dengan demikian, status strategis memperoleh legitimasi publik dan tidak digunakan untuk menutup proses kebijakan.

Integrated Maritime Defense Infrastructure Framework (IMDIF) yang Direvisi

Berdasarkan sintesis literatur, penelitian ini mengembangkan ulang Integrated Maritime Defense Infrastructure Framework (IMDIF). Versi revisi menempatkan Giant Sea Wall sebagai node dalam arsitektur pertahanan maritim sipil, bukan sebagai proyek adaptasi yang kemudian diberi label strategis. IMDIF terdiri atas lima lapisan yang saling terhubung.

Lapisan pertama adalah threat spectrum and securitization. Ancaman mencakup gangguan hidrometeorologis, kegagalan teknologi, ancaman asimetris dari arah perairan, sabotase, terorisme, gangguan terhadap fasilitas kritis, serta serangan siber. Sekuritisasi berfungsi untuk menentukan kapan gangguan tersebut memiliki konsekuensi strategis terhadap keselamatan masyarakat, kontinuitas fungsi vital, dan keamanan negara.

Lapisan kedua adalah physical and operational protection. Giant Sea Wall diposisikan bersama sistem penghalang, zona aman, kontrol akses, pengawasan, sensor, pemantauan, dan prosedur respons. Prinsipnya bukan mengubah seluruh struktur menjadi benteng, tetapi menerapkan perlindungan berbasis risiko pada critical nodes dan menggabungkan passive protection dengan active situational awareness.

Lapisan ketiga adalah critical function continuity. Fokusnya adalah pelabuhan, logistik, transportasi, energi, air, komunikasi, pelayanan darurat, dan fungsi pemerintahan. Ukuran keberhasilan bukan sekadar tidak adanya kerusakan fisik, tetapi kemampuan mempertahankan fungsi minimum, memiliki redundansi, dan memulihkan layanan dalam waktu yang dapat diterima.

Lapisan keempat adalah multi-agency command, control, and information fusion. Lapisan ini menghubungkan operator teknis, pemerintah, pelabuhan, penegak hukum, unsur keamanan, lembaga pertahanan, layanan kedaruratan, dan operator infrastruktur lain. Elemen intinya adalah common operating picture, protokol berbagi informasi, pembagian kewenangan, latihan bersama, dan prosedur eskalasi.

Lapisan kelima adalah cyber and institutional resilience. Lapisan ini mencakup keamanan teknologi operasional, kontrol akses, segmentasi jaringan, redundansi komunikasi, backup, mode manual, pemulihan, pembiayaan siklus hidup, akuntabilitas, dan evaluasi berkala. Lapisan ini memastikan bahwa sistem tidak hanya aman pada saat dibangun, tetapi tetap mampu beroperasi dalam jangka panjang dan menghadapi perubahan ancaman.

Secara konseptual, hubungan IMDIF dapat dirumuskan sebagai berikut: spektrum ancaman dan sekuritisasi → perlindungan fisik dan operasional → kontinuitas fungsi kritis → integrasi komando-kendali dan informasi → resiliensi siber serta kelembagaan → ketahanan wilayah dan dukungan terhadap pertahanan maritim. Kerangka ini membatasi klaim pertahanan pada fungsi yang dapat diuji, yaitu protection, continuity, awareness, coordination, dan recovery.

Tabel 2. Lapisan Integrated Maritime Defense Infrastructure Framework (IMDIF)

Lapisan	Fokus	Komponen utama	Outcome
1. Threat spectrum & securitization	Identifikasi ancaman strategis	Ancaman alam, asimetris, sabotase, cyber, technological failure	Prioritas risiko dan trigger respons
2. Physical & operational protection	Perlindungan titik kritis	Barrier, access control, surveillance, sensor, graded response	Mengurangi peluang dan dampak gangguan

Lapisan	Fokus	Komponen utama	Outcome
3. Critical function continuity	Menjaga layanan vital	Pelabuhan, logistik, energi, komunikasi, transportasi, layanan publik	Continuity, redundancy, recovery
4. Multi-agency C2 & information fusion	Koordinasi lintas lembaga	Common operating picture, data sharing, SOP, latihan, eskalasi	Respons terpadu dan cepat
5. Cyber & institutional resilience	Ketahanan sistem dan tata kelola	SCADA security, network segmentation, backup, manual mode, pembiayaan, audit	Operasi aman dan berkelanjutan

Strategi Pengembangan Giant Sea Wall sebagai Infrastruktur Pertahanan Maritim Strategis

Pertama, menetapkan klasifikasi fungsi strategis dan critical nodes. Pemerintah perlu memetakan bagian sistem yang apabila gagal akan menimbulkan konsekuensi besar terhadap pelabuhan, logistik, energi, komunikasi, transportasi, atau keselamatan publik. Pemetaan tersebut menjadi dasar diferensiasi standar perlindungan dan investasi keamanan.

Kedua, membangun layered waterside and infrastructure protection. Pengamanan tidak hanya berfokus pada kekuatan struktur, tetapi juga akses, perimeter, pengawasan, zona aman, dan perlindungan fasilitas kendali. Prinsip dari Kiciński et al. (2019) dan Giraud et al. (2011) dapat digunakan sebagai rujukan konseptual untuk memisahkan fungsi barrier, detection, assessment, dan response.

Ketiga, membentuk mekanisme multi-agency command and control. Diperlukan pusat atau mekanisme koordinasi yang mampu mengintegrasikan informasi teknis, keselamatan, keamanan, pelabuhan, penegakan hukum, dan pertahanan. Modelnya tidak harus meniru Joint Harbor Operations Center, tetapi perlu mengadopsi prinsip common operating picture, liaison, intelligence fusion, dan latihan bersama sebagaimana ditekankan Watts (2005).

Keempat, menerapkan cybersecurity by design. Seluruh sistem digital dan teknologi operasional harus masuk dalam risk assessment sejak tahap desain. Segmentasi jaringan, autentikasi, logging, backup, cadangan komunikasi, mode operasi manual, dan latihan insiden perlu dijadikan persyaratan desain dan operasi, sejalan dengan tantangan keamanan siber maritim yang diidentifikasi Cichocki dan Wójcik (2025).

Kelima, mengembangkan continuity of operations dan recovery plan lintas sektor. Operator pelabuhan, energi, telekomunikasi, transportasi, dan layanan publik harus memiliki rencana yang kompatibel. Latihan perlu menguji kombinasi skenario, misalnya gangguan fisik yang disertai kehilangan komunikasi atau kegagalan sistem kendali, sehingga kelemahan interdependensi dapat ditemukan sebelum krisis.

Keenam, menjamin kelembagaan, pembiayaan siklus hidup, dan legitimasi publik. Pelajaran Delta Works menunjukkan pentingnya komitmen jangka panjang, transparansi, dan penerimaan masyarakat (Lievonne et al., 2025). Status strategis Giant Sea Wall harus disertai anggaran operasi dan pemeliharaan, audit keandalan, indikator kinerja, keterbukaan peran lembaga, dan batas yang jelas antara pengelolaan sipil dan dukungan pertahanan.

Ketujuh, menerapkan adaptive security governance. Spektrum ancaman berubah lebih cepat daripada umur infrastruktur. Karena itu, standar keamanan dan IMDIF perlu ditinjau berkala berdasarkan perubahan teknologi, pola ancaman, insiden, hasil latihan, dan perkembangan sistem maritim. Infrastruktur strategis tidak boleh bergantung pada desain keamanan yang statis.

Implikasi Teoretis dan Keterbatasan Penelitian

Artikel ini memberikan dua implikasi teoretis. Pertama, sekuritisasi pertahanan pesisir dapat diperluas dari pembahasan ancaman lingkungan menuju pembahasan fungsi strategis infrastruktur. Suatu seawall menjadi relevan bagi pertahanan bukan karena bentuk fisiknya menyerupai fortifikasi, tetapi karena ia melindungi dan menopang sistem yang penting bagi keamanan nasional. Kedua, konsep critical infrastructure protection menunjukkan bahwa pertahanan maritim harus dipahami sebagai sistem sosio-teknis. Kekuatan struktur, sensor, jaringan digital, operator, regulasi, lembaga, dan koordinasi membentuk satu kesatuan; kegagalan pada salah satu unsur dapat mengurangi nilai perlindungan keseluruhan.

Penelitian ini memiliki keterbatasan. Pertama, IMDIF merupakan kerangka konseptual dan belum diuji melalui simulasi teknis Giant Sea Wall. Kedua, artikel tidak melakukan vulnerability assessment pada lokasi spesifik sehingga tidak menentukan perangkat pengamanan, jarak, sensor, atau konfigurasi operasional tertentu. Ketiga, kajian belum menguji struktur kewenangan lembaga Indonesia secara empiris. Penelitian lanjutan diperlukan melalui expert interview, tabletop exercise, pemodelan interdependensi infrastruktur, cyber risk assessment, serta analisis kelembagaan untuk menguji kelayakan setiap lapisan IMDIF.

5. SIMPULAN DAN SARAN

Giant Sea Wall Jakarta memiliki potensi untuk dikembangkan sebagai infrastruktur sipil strategis yang mendukung pertahanan maritim, tetapi nilai pertahanannya tidak berasal semata-mata dari fungsi tanggul sebagai penghalang air. Nilai tersebut muncul ketika Giant Sea Wall menjadi bagian dari sistem perlindungan yang menjaga kontinuitas pelabuhan, logistik, energi, komunikasi, transportasi, pelayanan publik, dan fungsi strategis lain di kawasan pesisir.

Orientasi tersebut memerlukan pergeseran dari proyek konstruksi menuju arsitektur keamanan dan resiliensi. Literatur mengenai maritime critical infrastructure protection menunjukkan pentingnya multi-agency command and control dan information fusion; kajian perlindungan fasilitas maritim menunjukkan perlunya layered physical protection dan surveillance; sementara perkembangan digital menempatkan cybersecurity sebagai bagian langsung dari keselamatan dan kontinuitas operasi. Pembelajaran Delta Works menambahkan bahwa sistem pertahanan pesisir hanya berkelanjutan apabila ditopang kelembagaan, transparansi, partisipasi, dan komitmen jangka panjang.

IMDIF yang direvisi mengintegrasikan lima lapisan, yaitu spektrum ancaman dan sekuritisasi, perlindungan fisik dan operasional, kontinuitas fungsi kritis, integrasi komando-

kendali dan informasi, serta resiliensi siber dan kelembagaan. Kerangka tersebut mempertahankan batas bahwa Giant Sea Wall bukan instalasi militer, namun membuka ruang bagi desain dual-use yang meningkatkan keandalan, situational awareness, koordinasi, dan recovery. Dengan demikian, kebijakan Giant Sea Wall dapat dikembangkan tidak hanya untuk mengurangi risiko pesisir, tetapi juga untuk memperkuat ketahanan wilayah dan mendukung pertahanan maritim Indonesia secara proporsional.

6. DAFTAR RUJUKAN

Kutipan artikel

Cichocki, R., & Wójcik, P. (2025). Cybersecurity in maritime transport systems: Threats, trends, and countermeasures in the last decade. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 19(3), 715–722. https://doi.org/10.12716/1001.19.03.03

Garschagen, M., Surtiari, G. A. K., & Harb, M. (2018). Is Jakarta's new flood risk reduction strategy transformational? Sustainability, 10(8), 2934. https://doi.org/10.3390/su10082934

Giraud, M.-A., Alhadef, B., Guarnieri, F., Napoli, A., Bottala-Gambetta, M., Chaumartin, D., Philips, M., Morel, M., Imbert, C., Itcia, E., Bonacci, D., & Michel, P. (2011). SARGOS: Securing offshore infrastructures through a global alert and graded response system. MAST Europe 2011 – Maritime System and Technology, 7th Global Conference & Exhibition, Marseille, France. HAL-00660219.

Kiciński, R., Jurczak, W., & Jabłońska, M. (2019). Technical aspect concerning vessels halt safety upon terrorist hazard. Journal of KONBiN, 49(2), 161–172. https://doi.org/10.2478/jok-2019-0030

Lievonne, M. C., Timur, F. G. C., & Hadianto, M. (2025). Securitization of coastal defense in the Delta Works projects: Lesson learned for Indonesia. KEMUDI: Jurnal Ilmu Pemerintahan, 9(2), 63–77. https://doi.org/10.31629/kemudi.v9i2.7072

Little, R. G. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. Journal of Urban Technology, 9(1), 109–123. https://doi.org/10.1080/106307302317379855

Morris, L. (2020). Stakeholder collaboration as a pathway to climate adaptation at coastal ports. Maritime Policy & Management, 47(7), 953–967. https://doi.org/10.1080/03088839.2020.1729435

Ninkovic, V. (2021). Critical infrastructure resilience: National approaches in the United States of America, the United Kingdom and Australia. Zbornik Radova Pravnog Fakulteta, Novi Sad. https://doi.org/10.5937/zrpfns55-30333

Nurhidayah, L., Davies, P., Alam, S., Saintilan, N., & Triyanti, A. (2022). Responding to sea level rise: Challenges and opportunities to govern coastal adaptation strategies in

Indonesia. Maritime Studies, 21, 339–352. https://doi.org/10.1007/s40152-022-00274-1

Takagi, H., Fujii, D., Esteban, M., & Yi, X. (2017). Effectiveness and limitation of coastal dykes in Jakarta: The need for prioritizing actions against land subsidence. Sustainability, 9(4), 619. https://doi.org/10.3390/su9040619

Watts, R. B. (2005). Maritime critical infrastructure protection: Multi-agency command and control in an asymmetric environment. Homeland Security Affairs, 1(2), Article 3.

Kutipan Buku

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.