Digitalisasi Martim: Mewujudkan Keamanan Laut Menuju Poros Maritim Dunia

Zani Susanto [1*], Anak Agung Istri Sri Wahyuni[2], Zulfa Maulida Nur Hafidzah[2]
[1]Nahkoda kapal
[2]Dosen

Email*: zanisusanto@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengkaji bagaimana digitalisasi sektor maritim dapat memperkuat sistem keamanan dan keselamatan laut Indonesia dalam rangka mewujudkan visi Indonesia sebagai poros maritim dunia. Metode penelitian yang digunakan adalah pendekatan kualitatif melalui studi pustaka (library research) dengan menganalisis literatur ilmiah, kebijakan pemerintah, laporan lembaga, dan sumber media terpercaya. Hasil penelitian menunjukkan bahwa Indonesia menghadapi tantangan keamanan maritim yang kompleks, baik dari sisi ancaman fisik seperti perompakan dan penangkapan ikan ilegal, maupun dari sisi ancaman digital seperti serangan siber terhadap sistem pelabuhan dan institusi keamanan laut. Kebaruan dalam penelitian ini terletak pada integrasi analisis antara ancaman fisik dan non-fisik sebagai satu kesatuan strategi pertahanan maritim. Penelitian ini merekomendasikan perlunya penguatan infrastruktur digital, peningkatan kapasitas sumber daya manusia, dan integrasi sistem informasi lintas lembaga. Implikasi temuan ini mendukung pentingnya perumusan kebijakan keamanan maritim berbasis digital yang adaptif, kolaboratif, dan berkelanjutan.
Kata kunci : Keamanan Maritim, Digitalisasi, Poros Maritim

Pendahuluan

Sebagai negara kepulauan terbesar di dunia dengan lebih dari 17.000 pulau, Indonesia memiliki posisi yang sangat strategis dalam jalur perdagangan internasional dan kepentingan geopolitik global. Namun, posisi ini juga menjadikan Indonesia rentan terhadap berbagai ancaman keamanan dan keselamatan maritim. Salah satu tantangan utama adalah maraknya kasus perompakan dan pelanggaran wilayah laut. Sepanjang tahun 2023, tercatat 55 kasus perompakan terjadi di wilayah perairan Indonesia, dengan 38 kasus di antaranya berlangsung di Selat Singapura, salah satu jalur pelayaran tersibuk di dunia (Deras News, 2024). Selain itu, ancaman dari kapal asing yang melakukan penangkapan ikan ilegal di perairan Indonesia juga masih menjadi masalah serius, terutama di wilayah Laut Natuna Utara. Indonesia Ocean Justice Initiative (2024) mencatat kehadiran kapal berbendera asing, termasuk dari Vietnam dan Tiongkok, yang melakukan pelanggaran di Zona Ekonomi Eksklusif (ZEE) Indonesia.

Di era digital, ancaman terhadap keamanan maritim tidak hanya bersifat fisik, tetapi juga non-fisik melalui serangan siber yang menargetkan sistem navigasi, pelabuhan, dan institusi maritim nasional. Pada tahun 2024, Badan Keamanan Laut (Bakamla) melaporkan bahwa mereka menerima lebih dari 23 juta serangan siber, termasuk insiden malware pada 1 Agustus 2024 yang menyebabkan gangguan terhadap jaringan internal lembaga tersebut

(Itworks.id, 2024). Lebih luas lagi, serangan ransomware terhadap Pusat Data Nasional (PDN) milik Kementerian Komunikasi dan Informatika pada Juni 2024 mengunci data dari 282 kementerian, lembaga, dan pemerintah daerah, serta mengganggu layanan publik seperti imigrasi dan tata kelola pemerintahan. Estimasi kerugian dari serangan tersebut mencapai Rp700 miliar (Reddit, 2024).

Menanggapi situasi tersebut, pemerintah telah mengambil beberapa langkah strategis, seperti penerbitan Surat Edaran Dirjen Perhubungan Laut Nomor SE-DJPL 16 Tahun 2024 yang mewajibkan setiap pelabuhan dan kapal untuk memiliki prosedur mitigasi risiko siber sesuai standar ISPS Code internasional (ShippingCargo.co.id, 2024). Selain itu, Kementerian Perhubungan bersama mitra internasional seperti Amerika Serikat telah mengadakan pelatihan keamanan digital maritim untuk melindungi pelabuhan otomatis seperti Terminal Teluk Lamong dari potensi serangan siber (Antaranews, 2024). Berbagai data dan peristiwa tersebut menunjukkan bahwa keamanan dan keselamatan maritim Indonesia saat ini tidak hanya tergantung pada kekuatan militer atau patroli laut, tetapi juga pada kemampuan untuk mengintegrasikan teknologi digital dalam sistem pengawasan dan pertahanan maritim. Transformasi digital maritim yang adaptif dan tangguh sangat diperlukan untuk menjawab tantangan era baru, sekaligus mendukung cita – cita besar Indonesia sebagai poros maritim dunia yang aman, inovatif, dan berkelanjutan.

Kesenjangan Penelitian

Kajian mengenai keamanan dan keselamatan maritim telah dilakukan oleh sejumlah peneliti baik di tingkat nasional maupun internasional. Nurhidayat (2019) dalam penelitiannya menyoroti peran strategis TNI Angkatan Laut dalam menjaga kedaulatan laut Indonesia melalui operasi patroli rutin dan penguatan kerjasama antar-lembaga. Penelitian ini menekankan pentingnya aspek militer dalam menjaga keamanan maritim, tetapi belum membahas integrasi teknologi digital secara mendalam. Rachman (2021) melakukan studi tentang pemanfaatan sistem Automatic Identification System (AIS) dalam pengawasan pergerakan kapal di wilayah perairan Indonesia. Ia menyimpulkan bahwa AIS mampu meningkatkan deteksi dini terhadap kapal-kapal ilegal, namun terdapat kendala dalam implementasi menyeluruh di daerah terpencil karena keterbatasan infrastruktur digital dan koordinasi antarinstansi.

Sementara itu, studi oleh Sibarani & Hafid (2022) mengevaluasi kesiapan pelabuhan-pelabuhan di Indonesia terhadap ancaman serangan siber. Penelitian ini menyoroti lemahnya sistem proteksi data serta absennya prosedur tanggap darurat terhadap insiden digital di sektor transportasi laut. Di tingkat internasional, Bueger (2015) mengembangkan konsep maritime security yang mencakup ancaman fisik dan non – fisik, serta pentingnya kolaborasi antaraktor negara dan non – negara untuk menciptakan keamanan laut yang holistik dan berkelanjutan. Namun, sebagian besar studi tersebut masih berdiri sendiri – sendiri antara aspek pertahanan, teknologi informasi, dan tata kelola tanpa mengintegrasikan ketiganya secara utuh dalam konteks transformasi digital maritim.

Berdasarkan tinjauan tersebut, dapat diidentifikasi adanya research gap pada pengkajian interseksi antara keamanan maritim dan sistem digital secara terpadu, khususnya dalam kerangka transformasi Indonesia menuju poros maritim dunia. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan tersebut dengan pendekatan yang lebih interdisipliner dan aplikatif.

Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisis kondisi aktual keamanan maritim Indonesia, mengidentifikasi tantangan dan peluang digitalisasi, serta merumuskan strategi integratif guna mendukung transformasi menuju poros maritim dunia.

Literature Review

Digitalisasi dalam Sektor Maritim

Digitalisasi maritim mencakup pemanfaatan teknologi informasi dan komunikasi (TIK) dalam sistem pelayaran, logistik, pengawasan laut, serta pengelolaan pelabuhan. Menurut Schinas & von Westarp (2017), digitalisasi maritim tidak hanya meningkatkan efisiensi operasional, tetapi juga menjadi instrumen utama dalam meningkatkan ketahanan sektor pelayaran dari ancaman kejahatan siber dan pelanggaran hukum laut. Teknologi seperti Automatic Identification System (AIS), radar satelit, big data analytics, dan sistem pelabuhan pintar (smart port) merupakan wujud dari transformasi digital ini.

Keamanan dan Keselamatan Maritim

Keamanan maritim merupakan komponen penting dalam menjaga kedaulatan negara dan kelancaran arus logistik laut. Bueger (2015) menyatakan bahwa keamanan maritim mencakup perlindungan terhadap kegiatan pelayaran, penegakan hukum di laut, pengendalian perbatasan maritim, serta pencegahan kejahatan transnasional. Dalam konteks Indonesia, tantangan keamanan laut mencakup perompakan, IUU fishing, penyelundupan, dan konflik batas maritim. Keselamatan maritim juga mencakup aspek teknis dan prosedural dalam mencegah kecelakaan laut dan kerusakan lingkungan.

Ancaman Siber di Sektor Maritim

Dengan meningkatnya penggunaan sistem digital, sektor maritim menjadi semakin rentan terhadap serangan siber. International Maritime Organization (IMO) telah mengeluarkan Guidelines on Maritime Cyber Risk Management untuk mendorong pelaku industri pelayaran dan pemerintah menerapkan sistem keamanan digital. Menurut Itworks.id (2024), Bakamla mencatat lebih dari 23 juta serangan siber yang menargetkan infrastruktur mereka dalam satu tahun terakhir, termasuk insiden malware dan penguncian sistem. Hal ini menunjukkan bahwa sistem keamanan digital harus menjadi prioritas dalam transformasi maritim nasional.

Transformasi Martim dan Visi Poros Maritim Dunia

Visi Indonesia sebagai poros maritim dunia pertama kali dicanangkan oleh Presiden Joko Widodo pada tahun 2014, yang menekankan pentingnya pembangunan sektor kelautan dan perhubungan laut sebagai pilar ekonomi nasional. Lima pilar utama dalam visi tersebut meliputi pembangunan budaya maritim, pengelolaan sumber daya kelautan, pembangunan infrastruktur dan konektivitas maritim, diplomasi maritim, dan penguatan pertahanan laut (Kemenko Marves, 2020). Dalam konteks ini, digitalisasi menjadi kunci dalam mewujudkan sistem transportasi laut yang efisien, aman, dan berdaya saing tinggi.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka *(library research)*. Pendekatan ini dipilih karena topik yang dikaji lebih bersifat konseptual dan

normatif, yaitu mengenai keamanan dan keselamatan maritim di era digital dalam konteks transformasi maritim Indonesia. Penelitian ini tidak mengandalkan data empiris lapangan, melainkan menekankan pada analisis kritis terhadap literatur, regulasi, dokumen kebijakan, laporan institusi, serta artikel jurnal yang relevan.

Sumber Data

Sumber data dalam penelitian ini berasal dari:

1. Literatur ilmiah, seperti jurnal nasional dan internasional, buku referensi, serta artikel akademik terkait topik keamanan maritim, digitalisasi sektor pelayaran, dan transformasi kebijakan maritim.
2. Dokumen resmi, termasuk regulasi pemerintah (misalnya SE-DJPL 16/2024), laporan tahunan lembaga seperti Bakamla, Kementerian Perhubungan, dan laporan dari organisasi internasional seperti IMO dan Ocean Justice Initiative.
3. Berita dan laporan media terpercaya, yang memberikan data kontekstual dan isu-isu terkini terkait serangan siber, pelanggaran wilayah, serta implementasi teknologi maritim.

Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui penelusuran dokumen dan literatur digital dari berbagai repositori online seperti Google Scholar, ResearchGate, jurnal SINTA, serta situs web resmi pemerintah dan lembaga keamanan maritim. Penelusuran ini dilakukan secara sistematis dengan kata kunci seperti: “keamanan maritim Indonesia”, “serangan siber pelabuhan”, “digitalisasi pelayaran”, “kebijakan keamanan laut”, dan “transformasi maritim Indonesia”.

Teknik Analisis Data

Analisis data dilakukan dengan teknik analisis isi (*content analysis*). Langkah-langkahnya meliputi:

1. Identifikasi tema-tema pokok dari berbagai sumber literatur yang relevan.
2. Klasifikasi informasi berdasarkan subtopik utama: kondisi aktual, tantangan digital, kebijakan yang ada, dan usulan strategi.
3. Interpretasi data secara kritis dan komparatif untuk menemukan keterkaitan antar konsep serta menyusun narasi yang koheren.
4. Simpulan, berupa rekomendasi kebijakan dan arah strategis untuk memperkuat keamanan maritim Indonesia di era digital.

Hasil dan Pembahasan

Hasil Penelitian

Berdasarkan studi pustaka yang dilakukan terhadap berbagai literatur ilmiah, laporan lembaga pemerintah, serta data media terpercaya, ditemukan beberapa hasil utama yang menjawab rumusan masalah dalam penelitian ini:

Kondisi Keamanan dan Keselamatan Maritim Indonesia di Era Digital

Keamanan maritim Indonesia masih menghadapi tantangan serius, baik dari ancaman fisik maupun non-fisik. Kasus perompakan laut yang masih marak, pelanggaran ZEE oleh kapal asing, serta penyelundupan menjadi isu utama yang terus berulang. Di sisi lain, era digital telah memperluas dimensi ancaman melalui serangan siber. Misalnya, pada tahun 2024, Bakamla mencatat lebih dari 23 juta serangan siber terhadap jaringan mereka (Itworks.id, 2024). Sementara itu, serangan ransomware terhadap Pusat Data Nasional pada

Juni 2024 menyebabkan gangguan pada layanan publik, termasuk sektor maritim (Reddit, 2024).

Tantangan dan Peluang Teknologi Digital dalam Keamanan Maritim

Tantangan utama dalam digitalisasi keamanan maritim meliputi keterbatasan infrastruktur komunikasi laut, lemahnya interoperabilitas data antar-lembaga, serta kurangnya sumber daya manusia yang terlatih dalam keamanan siber. Di sisi lain, peluang besar juga terbuka melalui pemanfaatan teknologi seperti Automatic Identification System (AIS), radar berbasis satelit, serta sistem berbasis kecerdasan buatan (AI) untuk mendeteksi aktivitas mencurigakan di perairan.

Strategi Integratif untuk Penguatan Keamanan Maritim Digital

Strategi yang efektif harus mencakup penguatan regulasi, peningkatan kapasitas personel, integrasi teknologi antar-instansi, serta peningkatan kerja sama internasional. Surat Edaran Dirjen Perhubungan Laut No. SE-DJPL 16 Tahun 2024 menjadi contoh kebijakan awal yang mendorong penerapan sistem keamanan siber di sektor pelabuhan dan perkapalan (ShippingCargo.co.id, 2024). Selain itu, pelatihan keamanan digital dengan negara mitra seperti Amerika Serikat juga merupakan langkah positif dalam memperkuat kesiapan nasional (Antaranews, 2024).

Jenis Ancaman	Bentuk Kasus	Strategi Mitigasi
Perompakan laut	55 kasus perompakan di 2023 (Deras News)	Patroli rutin, kerjasama lintas negara
IUU Fishing	Kapal asing di Natuna (IOJI, 2024)	Pemanfaatan AIS, penguatan diplomasi ZEE
Serangan Siber	Malware Bakamla & ransomware PDN (2024)	Audit keamanan TI, sistem back-up terdistribusi
Penurunan kualitas SDM TI	Rendahnya pelatihan personel maritim	Pelatihan intensif, kerja sama multinasional

Sumber: Penulis (2025)

Pembahasan

Hasil penelitian menunjukkan bahwa keamanan dan keselamatan maritim Indonesia tidak lagi bisa hanya ditangani melalui pendekatan konvensional seperti patroli laut dan penegakan hukum. Ancaman di era digital terutama yang bersifat non-fisik seperti serangan siber telah menjadi bagian tak terpisahkan dari sistem keamanan maritim modern. Hal ini sejalan dengan konsep comprehensive maritime security yang dikemukakan oleh Bueger (2015), di mana keamanan laut harus mencakup aspek militer, ekonomi, hukum, dan teknologi secara bersamaan.

Dalam konteks regional, Indonesia masih tertinggal dibandingkan negara-negara tetangga seperti Singapura, yang telah mengembangkan Maritime Cybersecurity Framework dan pusat operasi keamanan siber (CSOC) di pelabuhan-pelabuhan utama (IMDA, 2023). Hal ini menunjukkan adanya kebutuhan mendesak bagi Indonesia untuk mengadopsi model serupa yang berbasis koordinasi antarlembaga dan teknologi real-time.

Studi ini juga menemukan bahwa sebagian besar kebijakan keamanan maritim Indonesia masih bersifat sektoral dan belum sepenuhnya terintegrasi dalam satu platform

digital bersama. Kelemahan dalam interoperabilitas sistem informasi antara TNI AL, Bakamla, KKP, dan Kemenhub menghambat proses pengambilan keputusan yang cepat dan akurat. Hal ini diperkuat oleh temuan Rachman (2021) yang menyatakan bahwa sistem AIS belum diimplementasikan secara merata di seluruh wilayah perairan karena kendala infrastruktur dan minimnya pemantauan terpadu.

Dari sisi kebijakan, meskipun SE-DJPL 16 Tahun 2024 merupakan langkah awal yang progresif, namun pelaksanaannya masih menghadapi tantangan besar, terutama pada pelabuhan kecil dan daerah 3T (Tertinggal, Terdepan, dan Terluar) yang belum memiliki perangkat atau SDM yang memadai. Hal ini menunjukkan bahwa transformasi digital di sektor maritim memerlukan pendekatan bertahap, berbasis peta jalan nasional, dan melibatkan peran aktif pemerintah pusat, daerah, dan swasta.

Keterbatasan penelitian ini adalah keterbatasan akses terhadap data empiris dan teknis terkini dari institusi resmi seperti Bakamla, TNI AL, dan Kemenhub secara menyeluruh. Selain itu, karena bersifat studi pustaka, penelitian ini belum menyentuh pengalaman langsung dari pelaku di lapangan seperti operator pelabuhan, petugas keamanan laut, atau regulator. Oleh karena itu, studi lanjutan berbasis mixed-method yang menggabungkan data kualitatif dan kuantitatif di lapangan sangat diperlukan untuk memperdalam analisis serta menyusun rekomendasi kebijakan yang lebih praktis dan aplikatif.

Simpulan

Penelitian ini menyimpulkan bahwa keamanan dan keselamatan maritim Indonesia di era digital menghadapi tantangan yang semakin kompleks, baik dari sisi ancaman fisik seperti perompakan dan pelanggaran wilayah, maupun non-fisik seperti serangan siber terhadap infrastruktur pelabuhan dan sistem komunikasi laut. Transformasi digital telah membuka peluang signifikan melalui teknologi seperti AIS, radar satelit, dan kecerdasan buatan, namun belum diimbangi dengan kesiapan infrastruktur, integrasi sistem antarlembaga, serta kapasitas sumber daya manusia yang memadai.

Kebaruan (novelty) dari temuan ini terletak pada integrasi isu keamanan maritim dengan dimensi ancaman digital secara komprehensif, yang belum banyak dikaji dalam studi-studi sebelumnya secara utuh. Penelitian ini menekankan perlunya pendekatan kolaboratif lintas sektor dan lintas negara, serta urgensi pengembangan sistem keamanan maritim berbasis teknologi yang adaptif terhadap ancaman siber.

Implikasi dari penelitian ini menunjukkan bahwa untuk mewujudkan Indonesia sebagai poros maritim dunia, tidak cukup hanya dengan penguatan fisik armada laut atau kebijakan sektoral. Diperlukan langkah strategis jangka panjang berupa pembangunan infrastruktur digital maritim yang tangguh, peningkatan literasi siber bagi aparat dan operator pelabuhan, serta perumusan peta jalan keamanan maritim digital nasional yang terintegrasi. Temuan ini diharapkan menjadi dasar konseptual bagi pengambilan kebijakan dan studi lanjutan yang lebih aplikatif.

Daftar Pustaka

Antaranews. (2024). Kemenhub Lindungi Fasilitas Pelabuhan. https://antaranews.com

Bueger, C. (2015). What is Maritime Security?. Marine Policy, 53, 159–164. https://doi.org/10.1016/j.marpol.2014.12.005.

Deras News. (2024). Keamanan Maritim Indonesia Masih Lemah. https://derasnews.com.

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). Digital Era Governance: IT Corporations, the State, and E-government. Oxford University Press.

IMDA. (2023). Maritime Cybersecurity Framework. https://www.imda.gov.sg.

Indonesia Ocean Justice Initiative. (2024). Ancaman Keamanan Laut. https://oceanjusticeinitiative.org.

International Maritime Organization. (2017). Guidelines on Maritime Cyber Risk Management.

Itworks.id. (2024). Bakamla Gunakan AI untuk Pantau Aktivitas Maritim. https://www.itworks.id.

Kemenko Marves. (2020). Roadmap Poros Maritim Dunia 2045. Jakarta.

Nurhidayat, M. (2019). Peran TNI AL dalam Menjaga Kedaulatan Laut. Jurnal Pertahanan dan Bela Negara, 9(1), 34–47.

Rachman, D. (2021). Implementasi Sistem AIS dalam Pengawasan Laut Indonesia. Jurnal Transportasi Laut, 7(2), 112–125.

Reddit. (2024). Serangan Ransomware Pusat Data Nasional. https://www.reddit.com/r/indonesia.

Schinas, O., & von Westarp, A.G. (2017). Maritime Cybersecurity: A Holistic Approach. Springer.

ShippingCargo.co.id. (2024). SE-DJPL 16/2024. https://shippingcargo.co.id.

Sibarani, A., & Hafid, R. (2022). Kesiapan Pelabuhan terhadap Ancaman Siber. Jurnal Sistem Informasi Maritim, 5(1), 55–68.