MANDUB: Jurnal Politik, Sosial, Hukum dan Humaniora
Vol. 2 No. 1 Maret 2024
e-ISSN : 2988-2273, p-ISSN : 2988-2281, Hal 378-386
DOI: https://doi.org/10.59059/mandub.v2i1.940

Maritime Cybersecurity: Tantangan Dan Strategi Keamanan Maritim Indonesia

Saskia Aulia Putri
Universitas Hasanuddin

Agussalim Burhanuddin
Universitas Hasanuddin

Alamat: JI. Perintis Kemerdekaan No.KM.10, Tamalanrea Indah, Kec. Tamalanrea, Kota Makassar, Sulawesi Selatan 90245
Korespondensi penulis: kiasaskiaptr@email.com

Abstract. *The existence of digital transformation in the development of the world, makes the maritime industry increasingly rely on technology to carry out navigation, communication, and logistics intermediaries. As the maritime industry continues to adopt digitalization and adapt, the need for strategy as well as strengthening cybersecurity becomes critical for the country. The increase in cybercrime and its vulnerabilities should make Indonesia more aggressively address or anticipate this problem. Although it is proven that indonesia in its initiation of a cybersecurity strategy has increased, Indonesia is seen as still lacking to show the nation's commitment in terms of cyber security, when compared to data from NCIS (National Cyber security Index) from 2016-2023 Indonesia is still far below its neighbor, Malaysia, which is also a maritime country. Through a qualitative approach, this article aims to explain the urgency of cybersecurity in the maritime sector, highlighting challenges and solutions to protect ships, ports, and maritime infrastructure from cyber threats in Indonesia*.

Keywords: *Cyber, Indonesia, Maritime*

Abstrak. Adanya transformasi digital dalam perkembangan dunia, membuat industri maritim semakin mengandalkan teknologi untuk melakukan navigasi, komunikasi, dan perantara logistik. Saat industri maritim terus mengadopsi digitalisasi dan beradaptasi, kebutuhan akan strategi serta penguatan *cybersecurity* menjadi sangat penting bagi negara. Peningkatan kejahatan siber serta kerentanannya seharusnya membuat Indonesia lebih gencar mengatasi atau mengantisipasi masalah ini. Walau terbukti, indonesia dalam inisiasinya terhadap strategi keamanan siber mengalami peningkatan, Indonesia dipandang masih kurang menunjukkan komitmen bangsa dalam hal keamanan siber, jika dibandingkan melalui data dari *NCIS (National Cyber security Index)* dari tahun 2016-2023 Indonesia masih jauh dibawah negara tetangganya yaitu Malaysia yang juga termasuk negara maritim. Melalui pendekatan kualitatif, artikel ini bertujuan untuk menjelaskan urgensi keamanan siber dalam sektor maritim, yang menyoroti tantangan dan solusi untuk melindungi kapal, pelabuhan, dan infrastruktur maritim dari ancaman siber di negara Indonesia.

Kata kunci: Siber, Indonesia, Maritim.

PENDAHULUAN

Bagaimana seharusnya posisi Indonesia dalam menghadapi ancaman siber di industri maritim? Pertanyaan krusial seperti ini sudah sepatutnya muncul di era digital saat ini. Transformasi digital dalam perkembangan dunia, membuat perubahan besar diberbagai industri, termasuk industri maritim yang saat ini semakin mengandalkan teknologi untuk melakukan navigasi, komunikasi, dan perantara logistik. Ketika industri maritim terus mengimplementasi digitalisasi dan mulai menunjukkan sifat yang dependen, kebutuhan akan strategi serta penguatan *cybersecurity* menjadi hal krusial bagi setiap negara. Dalam konteks

Received: November 27, 2023; Accepted: Desember 28, 2023; Published: Maret 31, 2024
*Saskia Aulia Putri, kiasaskiaptr@email.com

Hubungan Internasional, Industri maritim penting karena menghasilkan bisnis yang menguntungkan negara dan banyak difungsikan untuk mempererat hubungan antar negara. Hal yang menguntungkan salah satunya dapat menyediakan lapangan kerja bagi puluhan ribu orang setiap hari. Maritim juga penting dalam hal ekonomi global karena menghubungkan berbagai benua secara bersamaan. Sebagian besar jalur perdagangan mengandalkan laut sebagai sarananya, maka hal ini menjadikan maritim sangat penting bagi perdagangan internasional.

PT Biro Klasifikasi Indonesia (Persero) sebagai satu-satunya BUMN yang bertanggung jawbab di bidang klasifikasi kapal dengan memainkan peran vital atas keselamatan angkutan moda laut berbendera Indonesia. Melalui pernyataan dari Direktur Utama PT Biro Klasifikasi Indonesia (Persero**)** Rudiyanto**,** terdapat banyak kerentanan yang bisa terjadi di atas kapal, seperti *Bridge systems, Cargo handling and management systems, Propulsion and machinery management and power control systems, Access control systems, Passenger servicing and management systems, Administrative and crew welfare systems, dan Communication systems*. Dari banyaknya celah yang bisa diretas, serangan-serangan juga datang dalam bentuk pembajakan. Maka dari itu, melindungi kapal, pelabuhan, serta seluruh infrastruktur maritim dari ancaman siber memerlukan pendekatan komprehensif yang mencakup solusi teknologi, kerangka regulasi, dan tenaga kerja maritim yang berwawasan.

KAJIAN TEORITIS

Maritim

Maritim memiliki beberapa definisi, yang setiap definisinya selalu berhubungan dengan kapal dan pelayaran, namun definisi yang paling umum ialah 'terhubung dengan laut’. Dalam konsteks maritim semua yang berhubungan dengan lautan, atau perahu apa pun yang berlayar di sepanjang permukaannya dianggap maritim, tidak peduli seberapa jauh perahu itu melakukan perjalanan ke pelosok.

Keamanan Siber

Keamanan siber adalah seni melindungi jaringan, perangkat, dan data dari akses tidak sah atau penggunaan kriminal, atau juga berarti sebuah praktik yang memastikan kerahasiaan, integritas, dan ketersediaan informasi.

Serangan Siber

Serangan siber adalah segala upaya yang disengaja untuk mencuri, mengekspos, mengubah, menonaktifkan, atau menghancurkan data, aplikasi, atau aset lain melalui akses ilegal ke jaringan, sistem komputer, atau perangkat digital.

METODE PENELITIAN

Pendekatan Penelitian

Pendekatan yang dipakai dalam penelitian ini merupakan pendekatan deskriptif kualitatif sehingga data yang dikumpulkan penulis dijabarkan menggunakan kata-kata atau kalimat. Kajian dilakukan dari sumber literatur seperti journal, report, maupun artikel dari sumber yang valid. Langkah-langkah kajian diawali dengan mengidentifikasi ancaman keamanan siber dilaut Indonesia, selanjutnya mengidentifikasi strategi pemerintah Indonesia yang telah berjalan dengan menganalisis poin-poin dalam NCIS framework melalui aspek masyarakat, regulasi, dan teknologi, terakhir mengusulkan rekomendasi untuk peningkatan implementasi strategi Indonesia di masa depan.

Tujuan Penelitian

Artikel ini bertujuan untuk menjelaskan urgensi keamanan *cyber* dalam sektor maritim, yang menyoroti tantangan dan solusi untuk melindungi kapal, pelabuhan, dan infrastruktur maritim dari ancaman siber negara Indonesia.

Manfaat Penelitian

Adapun manfaat dari artikel ini diharapkan dapat meningkatkan kesadaran di industri maritim akan adanya ancaman *cyber*, selain itu, temuan dari artikel ini dapat memberikan wawasan mengenai teknologi serta strategi keamanan *cyber* yang dapat diterapkan dalam operasi sehari-hari di industri maritim.

HASIL DAN PEMBAHASAN

Terminologi *Cybersecurity* Dalam Industri Maritim

Kemajuan teknologi dan kebangkitan ‘Internet’ telah mengubah masyarakat dan kehidupan kita secara kompleks. Kompleksitas yang berkembang mengubah kehidupan di seluruh dunia baik secara positif maupun negatif mulai dari segi sosial, politik, dan hukum yang kemudian memunculkan implikasi penting bagi keamanan, mengingat konektivitas digital juga dapat digunakan sebagai peluang untuk (1) mengubah distribusi kekuasaan, misal platform sosial media seperti Instagram dan Twitter, yang awalnya dirancang untuk menghubungkan teman dan keluarga melalui berbagi unggahan foto, video serta komen, menjadi titik fokus kontroversi pemilu (*Hoax, Black Campaign*, dll) dan pengaruh politik, (2) mencapai maksud yang bersifat koersif (Pemerasan, Penipuan, dll), (3) serta sebagai faktor yang berkontribusi terhadap kerentanan ancaman bagi negara atau suatu organisasi. Konflik siber dan perang siber telah menjadi isu yang cukup diperhatikan dalam ranah Hubungan Internasional. Disadari atau tanpa disadari dunia telah bergantung pada setiap kemajuan

teknologi, dan ketergantungan ini menciptakan persepsi kerentanan. Sehingga munculnya urgensi akan pentingnya keamanan siber sebagai isu dominan yang muncul dalam Hubungan Internasional, bukanlah tanpa sebab. Adanya ketergantungan yang semakin meningkat pada kemajuan teknologi dapat menciptakan suatu pandangan atau pemahaman bahwa keadaan tersebut menjadikan suatu sistem atau entitas menjadi rentan terhadap berbagai ancaman, seperti keamanan maritim yang muncul sebagai ancaman baru bagi suatu negara.

Dimensi keamanan nasional bertumpu pada perspektif yang memandang keamanan nasional sebagai upaya melindungi keberlangsungan negara sehingga fokus meningkatkan kekuatan laut negara ada pada kekuatan angkatan laut sebagai kekuatan yang dominan dalam konteks maritim. Atau dengan kata lain, keamanan maritim dianggap identik atau terkait erat dengan penggunaan kekuatan militer laut. Berbeda pandangan dengan Bueger yang menyatakan keamanan maritim tidak hanya terbatas pada aspek militer, tetapi mencakup empat konsep utama, yaitu (1) Keamanan Nasional, (2) Keamanan Ekonomi, (3) Keamanan Manusia dan (4) Lingkungan Laut.[1] Adapun bidang terkait yang mengancam keamanan maritim dalam lingkup keempat konsep ini bisa berupa sengketa maritim antar negara, terorisme maritim, dan penangkapan ikan ilegal. Terlepas dari semua hal diatas, tantangan modern terhadap keamanan maritim tidak hanya berasal dari ranah fisik, melainkan juga melibatkan ranah siber. Serangan siber merupakan upaya mencuri data atau menyebabkan kerusakan pada komputer, jaringan, atau perangkat dengan menggunakan metode yang bervariasi untuk membobol sistem komputer demi mencapai kepentingan pribadi, kriminal, dan politik.[2] Implikasinya pada dunia fisik dapat ditandai dengan munculnya Teknologi Operasional (OT) seperti sistem penanganan kargo di pelabuhan dan sistem kontrol mesin di atas kapal yang terhubung langsung ke internet.

Dalam terminologi *Maritime Cybersecurity* terdapat domain maritim yang melibatkan pengamanan *Critical Information Infrastructure* (CII) dimana sektor ini menjaga dari serangan siber atau dari kesalahan tidak disengaja lainnya yang dapat melumpuhkan, mengganggu, atau mengendalikannya sebuah kapal.[3] Di sektor perkapalan terdapat pula istilah yang diciptakan untuk menggambarkan keamanan siber maritim sebuah kapal yang disebut " *cyber seaworthiness*".[4] Istilah "*cyber seaworthiness*" digunakan untuk menggambarkan *maritime cybersecurity* sebuah kapal. Konsep tersebut menunjukkan bahwa keamanan siber telah masuk menjadi bagian integral dari kesiapan operasional sebuah kapal di era modern, di mana

[1] Bueger, C. "What is Maritime Security?" in Marine Policy (2014), pp. 4-5
[2] https://www.forbes.com/advisor/business/what-is-cyber-attack/
[3] Fitton, O., Prince, D., Germond, B. "The Future of Maritime Cyber Security" in Lancaster University (2015),p. 8.
[4] Gillespie, C. "Cyber Risks: Insurance Cover and Cyber Preparedness" in Safety4Sea (2018).

ancaman siber dapat memiliki dampak serius pada keseluruhan keberlanjutan dan keamanan operasional kapal.

Tantangan Keamanan Siber Indonesia Dalam Industri Maritim

Serangan siber merupakan ancaman yang muncul bagi sektor maritim. Meskipun komitmen nasional akan masalah ini belum sepenuhnya disadari, serangan siber menimbulkan ancaman yang berkelanjutan dan akan semakin memburuk seiring berjalannya waktu. Tidak seperti bajak laut yang tindakannya dapat terlihat dan dapat diamati secara langsung, ancaman dari dunia maya tidak melakukan interaksi fisik secara langsung sehingga serangan ini sulit untuk terlihat dan menggunakan berbagai cara untuk menjaga anonimitas mereka demi menutupi jejaknya. Semakin canggih sistem perkapalan dan semakin terotomatisasi sistemnya, semakin besar peluang untuk melakukan infiltrasi dan mencapai tujuan penyerang. pengelompokkan ancaman siber dibagi menjadi tiga, yang pertama, Peretas *nation-state* bertindak atas nama pemerintah mereka untuk mengkompromikan negara target, organisasi, atau individu demi mengumpulkan informasi intelijen atau menyebabkan kerusakan. Mereka biasanya memiliki sumber daya yang baik, sangat terampil dan tidak termotivasi oleh keuntungan uang. Peretas *nation-state* sering dikaitkan dengan serangan yang menyerang fasilitas industri yang menggunakan Teknologi Operasional (OT), atau yang dikenal sebagai Sistem Kontrol Industri. Sistem OT mencakup perangkat keras dan perangkat lunak yang memantau dan mengontrol perangkat dan proses fisik, termasuk sistem propulsi, sistem manajemen kargo, dan lainnya di atas kapal. Serangan siber pada sistem OT dapat mengakibatkan kerusakan fisik pada infrastruktur atau gangguan layanan penting. Dari banyaknya kasus peretasan sistem OT yang menyerang negara, salah satunya adalah kasus pada tahun 2017, dimana sistem instrumen keselamatan fasilitas minyak dan gas di Arab Saudi dinonaktifkan, yang mengakibatkan pembangkit tersebut tidak dapat beroperasi dengan aman jika terjadi bencana.

Terdapat banyak alasan atau motif pelaku ancaman siber untuk menyerang industri maritim indonesia, yang pertama adalah motivasi geopolitik. Lokasi strategis laut Indonesia di Asia Tenggara maupun di dunia, bersama dengan populasi dan potensi ekonominya yang besar, menjadikannya pemain penting dalam geopolitik regional dan global. pelaku menargetkan Indonesia untuk mendapatkan keuntungan dari sumber daya alamnya, mengganggu stabilitas regional, atau mengumpulkan informasi intelijen sehingga tingkat ketertarikan pelaku ancaman akan tinggi dan akan terus naik apabila strategi keamanan siber Indonesia tidak ditingkatkan. Kedua, penerapan sistem keamanan berteknologi di sektor maritim khususnya di atas kapal saat ini belum terlalu diperhitungkan. Perangkat sistem keamanan kapal Indonesia masih

kurang mumpuni, walaupun memang masih banyak kapal Indonesia yang belum berteknologi karena perangkat jaringan internet yang mahal dan bandwidth yang terbatas dikarenakan kapal berada ratusan atau ribuan mil dari daratan terdekat dimana konektivitas jaringan internet harus disediakan melalui satelit. Disisi lain, sebagian besar kapal kapal penting milik Indonesia atau kapal milik BUMN sudah menggunakan teknologi, namun dengan kurangnya perangkat keamanan yang mumpuni dapat membuka celah untuk para pelaku melakukan serangan siber. Ketiga, kurangnya Sumber Daya Manusia yang memiliki wawasan keamanan atau ancaman siber. Di Indonesia sendiri, menurut data dari NCIS yang diambil dari 28 April 2023, menunjukkan setidaknya hanya satu program yang berfokus pada keamanan siber / keamanan informasi elektronik di tingkat Sarjana atau setara yang terdapat hanya di Universitas Bina Nusantara. Faktor ini dapat menjadi indikator kurangnya upaya dalam mendidik dan melatih SDM di Indonesia di bidang keamanan siber. Dampaknya bisa menciptakan kesenjangan dalam ketersediaan tenaga ahli keamanan siber di tingkat nasional.

Strategi Nasional Maritim Indonesia Terhadap Serangan Siber

Pada tahun 2021, dalam upayanya untuk meningkatkan efektifitas strategi Indonesia akan ancaman siber, Presiden Joko Widodo memperkuat Badan Siber dan Sandi Negara (BSSN) Indonesia dengan mengeluarkan Peraturan Presiden Republik Indonesia nomor 28 tahun 2021 yang salah satunya berisi keputusan menempatkan BSS langsung di bawah naungan presiden alih-alih kementerian atau badan pemerintah lainnya dengan harapan dapat meningkatkan ketangkasan dan kewenangan BSSN. Indonesia juga sedang mengerjakan strategi keamanan siber nasional pertama kalinya, kerangka kerja pengelolaan krisis siber nasional, dan kerja sama bilateral dengan Pemerintah Australia dalam menangani keamanan siber di wilayah tersebut.[5] Namun terlepas dari upaya indonesia pada saat itu, upaya khusus dalam menangani serangan siber di industri maritim masih belum cukup.

Dalam kerangka kerja *National Cyber Security Index* (NCSI), pengembangan kebijakan keamanan siber dinilai dari beberapa aspek, yaitu yang **pertama** unit kebijakan keamanan siber. Penilaian tersebut berupa entitas pemerintah pusat (kementerian atau yang setara) memiliki unit khusus yang bertanggung jawab atas pengembangan kebijakan keamanan siber nasional. Di Indonesia, upaya pengembangan kebijakan keamanan siber diwujudkan dengan pembentukan Badan Siber Dan Sandi Negara (BSSN) sesuai dengan Keputusan Presiden No. 28 Tahun 2021. Dalam kunjungan menteri Koordinator Bidang Kemaritiman dan Investasi

[5] Keller-Nabbs, G., Wibawanto, R.M., & Widodo, N. "Indonesia Responds to the Cyber Dark Side", Lowy Institute (2021).

Luhut Binsar Pandjaitan di tahun 2020, BSSN memaparkan berbagai rencana dan capaian BSSN terkait pengembangan infrastruktur Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas), pengamanan Aplikasi Kritis Nasional, dan peningkatan cyberpower Indonesia diantaranya terkait dengan penguatan Kapasitas SDM Keamanan Siber, pembangunan dan penguatan Computer Emergency Response Team (CERT), perkembangan penyusunan RUU Keamanan dan Ketahanan Siber dan peraturan turunannya serta peningkatan kerjasama internasional di bidang keamanan siber.[6] Dari banyaknya rangkaian yang ingin dicapai, walau tidak secara spesifik membahas keamanan siber maritim.

Upaya BSSN mencakup substansi maritim. Yang dapat diartikan bahwa dalam upayanya untuk meningkatkan keamanan siber nasional, BSSN juga mempertimbangkan dan melibatkan isu-isu keamanan siber yang terkait dengan sektor maritim. Selanjutnya, dari aspek strategi keamanan siber. Penilaian pada aspek ini lebih kepada upaya Pemerintah pusat dalam menetapkan strategi keamanan siber tingkat nasional atau dokumen lain yang setara. Sayangnya, melalui data terakhir NCSI di tanggal 28 April 2023, tidak ditemukan strategi yang dimaksud namun Indonesia memiliki komunitas independen (CSIRT, CERT, CIRT, dll.) yang berspesialisasi dalam deteksi dan respons insiden dunia maya tingkat nasional seperti id.cert dan Id-SIRTII/CC. Begitu pula pada aspek rencana implementasi strategi keamanan siber dengan menilai upaya pemerintah pusat dalam menetapkan rencana implementasi strategi keamanan siber tingkat nasional atau dokumen lain yang setara. Dan terakhir ada pada aspek operasi siber militer. Pasukan militer Indonesia memiliki satu unit (komando siber, dll.) yang berspesialisasi dalam perencanaan dan pelaksanaan operasi dunia maya yaitu patroli siber. Pemerintah juga telah melakukan latihan manajemen krisis siber tingkat nasional atau latihan manajemen krisis dengan komponen siber dalam 3 tahun terakhir seperti program ”Gema Bhakti”. Tujuan latihan termasuk meningkatkan koordinasi kemampuan militer dengan badan-badan sipil dan komunitas bantuan kemanusiaan; mengorganisir dan mengintegrasikan ke dalam gugus tugas gabungan untuk melaksanakan operasi militer; dan meningkatkan pengembangan profesional melalui keamanan maritim bilateral, siber, dan acara perencanaan tingkat operasional lainnya.

Solusi Dalam Peningkatan Cybersecurity Maritim Di Indonesia

Sebagian besar kapal maritim yang dijalankan Indonesia menggunakan perangkat lunak yang sudah lama dan perangkat keras yang tidak dirancang dengan mempertimbangkan keamanan siber. Sehingga Langkah pertama yang harus dilakukan pemerintah Indonesia

[6] Redaksi. (2021). “Menjaga Keamanan Siber Maritim” di Logistik News

adalah dengan melakukan pembaruan pada sistem kapal yang sudah ada, misal memodifikasi sistem kapal agar mampu mendeteksi dan mencegah serangan siber atau merancang sistem kapal agar memiliki kemampuan untuk pulih dengan cepat dan efektif setelah mengalami serangan siber. Pembaruan sistem kapal bertujuan untuk memastikan bahwa teknologi yang digunakan tetap relevan, dan dapat menanggapi ancaman siber yang semakin canggih. Namun, pembaruan sistem kapal tidak selalu membutuhkan alat yang mewah atau lebih mahal dari sebelumnya, tetapi dapat dicapai dengan fokus pada peningkatan keamanan sistem kapal yang melibatkan perubahan pada konfigurasi keamanan, perlindungan terhadap *malware*, dan manajemen akses yang lebih ketat sehingga dapat menghemat anggaran. Selanjutnya, Peningkatan pelatihan dan kesadaran Sumber Daya Manusia (SDM) di sektor maritim Indonesia merupakan langkah krusial dalam memitigasi risiko ancaman siber. Dalam konteks ini, program pelatihan khusus keamanan siber dapat diselenggarakan, dengan mengutamakan aspek-aspek yang relevan dalam lingkungan kerja di sektor maritim. pelatihan tersebut dapat mencakup simulasi serangan siber, memberikan pengalaman praktis kepada SDM dalam menghadapi skenario serangan yang mungkin terjadi. Pendekatan edukasi berkelanjutan ini dapat membantu masyarakat Indonesia untuk terus meningkatkan pemahaman mereka terhadap ancaman siber.

KESIMPULAN DAN SARAN

Transformasi teknologi dan kebangkitan internet telah membuka celah baru dalam industri maritim. Ancaman siber menjadi tantangan serius dalam sektor maritim Indonesia. Meskipun telah ada upaya dan perubahan kebijakan, mulai pembentukan Badan Siber Dan Sandi Negara (BSSN) hingga munculnya organisasi independen di Indonesia untuk mengatasi ancaman siber, masih terdapat kekurangan dalam menangani ancaman siber terhadap industri maritim. Serangan siber dapat memiliki dampak yang signifikan terhadap keamanan nasional, ekonomi, dan operasional kapal. Tantangan utamanya meliputi kurangnya perhatian terhadap keamanan siber maritim, kurangnya implementasi teknologi keamanan di atas kapal, dan kurangnya sumber daya manusia yang terlatih dalam mengatasi ancaman siber. Indonesia perlu segera mengambil langkah-langkah strategis untuk mengatasi masalah ini. Peningkatan keamanan sistem kapal melalui pembaruan teknologi dan fokus pada keamanan konfigurasi, perlindungan terhadap malware, serta manajemen akses yang ketat dapat menjadi langkah awal yang efektif. Selain itu, peningkatan kesadaran terhadap ancaman siber di kalangan Masyarakat Indonesia menjadi kunci untuk memitigasi risiko. Program pelatihan khusus keamanan siber dapat memberikan pemahaman praktis dan simulasi serangan siber untuk meningkatkan

kesiapan SDM. Pemerintah perlu mempertimbangkan strategi keamanan siber yang lebih terfokus pada sektor maritim, termasuk perencanaan implementasi strategi keamanan siber dan operasi siber militer. Kolaborasi internasional juga dapat menjadi aspek penting dalam membangun keamanan siber yang efektif. Dengan mengambil langkah-langkah ini, diharapkan Indonesia dapat meningkatkan tingkat keamanan siber maritimnya, melindungi infrastruktur kritis, dan memastikan kelangsungan operasional yang aman di tengah ancaman yang terus berkembang di dunia maya.

DAFTAR REFERENSI

Bueger, C. *"What is Maritime Security?" in Marine Policy* (2014), pp. 4-5

Bueger, H (2015). "What is maritime security?", Marine Policy, Volume 53,Pages 159-164,https://doi.org/10.1016/j.marpol.2014.12.005.

Fitton, O., Prince, D., Germond, B. "*The Future of Maritime Cyber Security"* in Lancaster University (2015), p. 8.

Gillespie, C. "*Cyber Risks: Insurance Cover and Cyber Preparedness*" in Safety4Sea (2018).

Harknett, R.J., Callaghan, J.P., & Kauffman, R. (2010). *"Leaving Deterrence Behind: War-Fighting and National Cybersecurity".*

Joanna J. Bryson, Helena Malikova*; Is There an AI Cold War?*. Global Perspectives 1 February 2021; 2 (1): 24803. doi: https://doi.org/10.1525/gp.2021.24803.

Jones, K. D., Tam, K., & Papadaki, M. (2016). *Threats and impacts in maritime cyber security.*

Josephine Wolff; *How Is Technology Changing the World, and How Should the World Change Technology?*. Global Perspectives 1 February 2021; 2 (1): 27353. doi: https://doi.org/10.1525/gp.2021.27353.

Neo, M. (2021*). The Rising Threat of Maritime Cyber-attacks: Level of Maritime Cyber-security Preparedness along the Straits of Malacca and Singapore*. *Royal Australian Navy Sea Power*, (42), 38.

Redaksi. (2021). "Menjaga Keamanan Siber Maritim" di Logistik News

Sabova, N. (2021). *Cyber-worthiness: The duty to make the vessel seaworthy with respect to cybersecurity* (Master's thesis).

Shafran, D. (2023). "*What Does Maritime Mean?*" in Maritime Page.

Yan Jau, C. (2022). *"Cyber Attacks as an Evolving Threat to Southeast Asia's Maritime Security*.