MELAMPAUI KECEPATAN MESIN: ADAPTASI ROE DAN SINERGITAS DI ERA PERANG ATRIBUSI *ARTIFICIAL INTELLIGENT*

M. Imam Chadhafi
TNI Angkatan Laut
chadhafi070918@gmail.com
Efatha Filomeno Borromeu Duarte
Dosen Geostrategi dan Geopolitik FISIP Universitas Udayana
efathaborromeu@unud.ac.id
http://doi.org/10.52307/jmi.v912.200

A. PENDAHULUAN

Semboyan "Jalesveva Jayamahe" adalah mandat historis dan filosofis yang menempatkan penguasaan maritim sebagai *center of gravity* strategis Indonesia. Namun, pada dekade ketiga abad ke-21, domain maritim global telah bertransformasi dan secara historis didefinisikan oleh kontrol atas ruang fisik (Bueger, 2015). Domain tersebut telah berevolusi menjadi *datascape* yang kompleks, dimana 99% data global dan 80% perdagangan dunia bergantung pada integritas kabel bawah laut dan rute pelayaran (Talpur et al., 2025; Strobel, 2025). Sejalan dengan hal tersebut, diskursus strategis telah lama mengidentifikasi krisis adaptasi dan secara akurat mengobservasi bahwa konstruksi pertahanan kita saat ini masih terikat pada paradigma perang kemerdekaan, sehingga implementasi "Pertahanan Negara Kepulauan" masih terus dihadapkan dengan regulasi, doktrin maupun institusional (Salim, 2025).

Terdapat beberapa krisis yang menjadi dilema dan tantangan besar, dimana hal tersebut bukan sekadar kegagalan teknis, melainkan simptom dari penyakit kronis yang menghadirkan kegagalan dalam sistemik serta absensi akuntabilitas investigasi teknis yang transparan (CNBC Indonesia, 2021; Kumparan, 2021). Selain itu, tata kelola menjadi salah satu faktor yang menyebabkan konflik yurisdiksi maritim belum bisa terselesaikan dengan baik. Studi akademis (Jurnal UPY, 2023) mengonfirmasi bahwa penegakan hukum di laut belum terintegrasi dalam suatu Kodal yang terpusat dan masih bekerja secara sektoral. Namun perkembangan lingkungan strategis yang ada di level regional maupun global tidak membutuhkan waktu lama, karena *landscape* ancaman eksternal telah bertransformasi secara cepat. Musuh kontemporer tidak lagi mengandalkan platform fisik, namun mereka sudah mulai melancarkan "Perang Atribusi" dan mengubah perspektif menjadi sebuah

strategi hibrida yang secara presisi dirancang untuk mengeksploitasi krisis internal negara yang masih memiliki hambatan berupa "kendala doktrin" dan "ego sektoral". (Hoffman, 2009)

“Perang Atribusi” yang terjadi saat ini menggunakan akselerator utama yang dikenal dengan sebutan Kecerdasan Buatan (*Artificial Intelligent*/AI) (Horowitz, 2020; Allen, 2024). Kehadiran AI memungkinkan musuh untuk beroperasi pada kecepatan mesin (*machine speed*) (Johnson, 2023); meluncurkan serangan *non-atribusi* yang berkaitan dengan sabotase rantai pasok (*Middle East Monitor*, 2025); *spoofing* GPS (Data Q2 2025); dan serangan *firewall* (*The Record*, 2025), dimana seluruhnya dapat terjadi hanya dalam hitungan detik. Kondisi tersebut menjadi permasalahan sangat serius dan menghadirkan fakta bahwa "Kesenjangan Kecepatan" (*The Speed Gap*) adalah tantangan utama yang harus segera diselesaikan. Kesenjangan tersebut bukan hanya sekedar teori, namun telah terukur dan fakta tersebut dibuktikan dengan adanya respon *Network Centric Warfare* (NCW) dalam *Operation Iraqi Freedom* yang berjalan cepat dan membutuhkan waktu kurang dari 24 jam. Sedangkan di era AI, kecepatan tersebut NCW terbilang lambat, karena saat ini data operasional dari *"Project Ammo"* US *Navy* menunjukkan bahwa siklus adaptasi model AI di lapangan telah dipangkas dari enam bulan menjadi satu minggu (Cole, 2025).

Kesenjangan kecepatan yang terjadi akan semakin diperburuk dengan adanya friksi internal yang masih berkaitan dengan "ego sektoral" (Putri & Burhanuddin, 2023). Namun fenomena tersebut sebenarnya dapat diringkas dengan sempurna dalam forum C3 AI (2025) sebagai "*Artificial Intelligence* birokratis" dan menjadi metafora bagi puluhan orang untuk berdebat melalui *spreadsheet*. Selain itu, kondisi tersebut semakin menjelaskan bahwa kegagalan sistemik dalam penggunaan *Rules of Engagement* (ROE) masih mengarah pada kesenjangan relevansi yang dirancang untuk era konflik simetris dan atribusi yang jelas (Heuser, 2010). Sedangkan dengan adanya AI, maka tingkat kesulitan untuk merespon ancaman akan lebih tinggi karena terdapat keambiguan (Haase, 2025; Schmitt, 2019). Pada prinsipnya, ancaman hibrida yang ada saat ini memiliki fleksibilitas untuk menghancurkan musuh tanpa perlu menghancurkan alutsista, namun mereka hanya perlu meluncurkan serangan non-kinetik untuk melumpuhkan aspek teknis maupun non teknis yang tidak memiliki definisi hukum secara jelas dalam ROE.

Serangan tersebut berimplikasi pada fragmentasi yurisdiksi yang terjadi sebagai akibat dari "ego sektoral" dan "ketidakpastian hukum" yang diciptakan sendiri. Oleh karena itu, salah aspek yang perlu mendapatkan perhatian adalah efektivitas *Rules of Engagement* (ROE) maritim kontemporer yang saat ini sedang

ditantang secara fundamental oleh ancaman hibrida yang diakselerasi AI. Tantangan ini terjadi pada dua front, pertama tantangan eksternal (Atribusi), dimana AI mengaburkan identitas dan niat musuh (Maness & Valeriano, 2018); dan kedua adalah tantangan internal (Sinergi), dimana krisis tata kelola dapat menghambat respons keterpaduan *command and control*. Sehubungan dengan kondisi tersebut, maka artikel ini akan membahas tentang Kecerdasan Buatan (AI) yang secara fundamental dapat mengubah karakter ancaman hibrida maritim, sehingga menantang relevansi *Rules of Engagement* (ROE) konvensional pada pilar atribusi dan proporsionalitas. Kemudian membahas tantangan struktural internal di Indonesia khususnya "fragmentasi yurisdiksi" dan krisis yang dapat menghambat adaptasi serta kelincahan respons (*response agility*) dalam menghadapi "Perang Atribusi" yang bergerak pada kecepatan mesin.

B. METODE PENELITIAN

Artikel ini menggunakan desain kualitatif dengan pendekatan deskriptif-analitis. Desain ini dipilih karena tujuan penelitian bukanlah untuk mengukur frekuensi ancaman (kuantitatif), melainkan untuk memahami secara mendalam (*verstehen*) kompleksitas, konteks, dan implikasi doktrinal dari fenomena "Perang Atribusi" berbasis AI. Pendekatan deskriptif-analitis memungkinkan peneliti untuk membedah fenomena yang ada (ancaman AI dan krisis internal) dan menganalisisnya terhadap kerangka kerja normatif (doktrin dan ROE yang seharusnya).

Artikel ini disusun dengan menggabungkan 2 (dua) pendekatan utama, pertama studi Hukum-Doktrinal (*Doctrinal-Legal Research*) yang digunakan sebagai pendekatan untuk menganalisis teks otoritatif (*authoritative texts*) yang membentuk arsitektur keamanan maritim Indonesia. kemudian kedua adalah analisis studi kasus (*Case Study Analysis*) yang digunakan sebagai pendekatan hukum-doktrinal murni dan akan bersifat steril jika tidak divalidasi oleh realitas operasional. Oleh karena itu, artikel ini menggunakan pendekatan studi kasus komparatif (Yin, 2018). Studi kasus dipilih bukan untuk generalisasi statistik, melainkan untuk generalisasi analitis yaitu, untuk menguji dan memperkuat kerangka kerja teoritis ("Matriks Tiga Tantangan").

Teknik analisis data utama yang digunakan adalah *Gap Analysis*, dimana penulis memetakan "keadaan yang seharusnya" (*as-is*) yang didefinisikan oleh kerangka hukum-doktrinal Indonesia (ROE, UU RI tentang TNI dan Kelautan, UNCLOS 1982) ; "keadaan yang ada" (*to-be*) yang telah terdefinisikan oleh realitas ancaman hibrida berbasis AI (dari studi kasus OSINT); dan kendala internal (dari studi kasus krisis ancaman laut 2020-2025).

Secara spesifik, analisis akan dilakukan dengan. Selanjutnya limitasi dalam artikel ini adalah sangat bergantung pada sumber terbuka (OSINT) untuk menganalisis ancaman AI dan studi kasus asing. Kedua, teks lengkap *Rules of Engagement* (ROE) TNI yang berlaku saat ini merupakan dokumen rahasia negara dan tidak dapat diakses secara publik. Oleh karena itu, analisis terhadap "Tantangan ROE" didasarkan pada prinsip-prinsip ROE yang berlaku universal (misalnya, prinsip atribusi, proporsionalitas) dan doktrin hukum perang (LOAC) yang tersedia dalam literatur publik (Schmitt, 2019; Roscini, 2020).

C. PEMBAHASAN

Tantangan Atribusi (Menyerang Identitas dan Niat)

ROE konvensional diaktifkan oleh *hostile act* (tindakan bermusuhan) atau *hostile intent* (niat bermusuhan) yang teratribusi (Maness & Valeriano, 2018). Namun dengan kehadiran AI yang digunakan secara presisi berdampak pada atribusi yang menjadikan ROE tidak bisa digunakan. Ancaman yang ada saat ini tidak lagi datang dari rudal, tetapi dari *microchip*. Pada Oktober 2025, mantan Direktur Mossad, Yossi Cohen, secara terbuka mengakui strategi menanam "peralatan yang dimanipulasi mata-mata" (*spy-manipulated equipment*) di dalam rantai pasok musuh (*Middle East Monitor*, 2025). Secara paralel, terdapat kasus penjualan *cyber-exploits* ke broker Rusia (Bleeping Computer, 2025), dimana hal tersebut menunjukkan adanya pasar gelap yang matang untuk *insider threat* (ancaman orang dalam) di industri pertahanan.

Kondisi tersebut menjelaskan bahwa serangan dapat terjadi di luar yurisdiksi teritorial dan sebelum konflik dimulai (di masa damai). ROE lumpuh karena tidak ada *hostile act* yang jelas dari aktor negara yang teridentifikasi di dalam wilayah operasional. Sedangkan efek dari sabotase tersebut baru dirasakan setelah kerusakan terjadi, misalnya terjadinya kegagalan sistem tempur kapal saat dibutuhkan. Selanjutnya studi kasus kedua adalah terdapat laporan intelijen (Oktober 2025) yang mengidentifikasi grup peretas terkait Tiongkok, Storm-1849, secara aktif memindai dan mengeksploitasi *firewall* Cisco ASA (The Record, 2025). Kondisi tersebut membawa ke arah *grey zone* klasik. Serangan ini dapat dengan mudah disangkal (*plausible deniability*) dan disamarkan sebagai aktivitas kriminal non-negara. Sedangkan ROE tidak dirancang untuk mengotorisasi respons militer terhadap serangan siber yang tidak dapat diatribusi secara pasti ke aktor negara (Schmitt, 2019).

Tantangan Yurisdiksi (Menyerang Celah Birokrasi)

ROE terfragmentasi berdasarkan yurisdiksi lembaga, sedangkan ancmaan hibrida telah mengeksploitasi kondisi

tersebut dengan meluncurkan serangan yang secara sengaja tidak jelas yurisdiksinya (Klein, 2021). Stusdi kasus pertama terjadi pada Infrastruktur *Dual-Use* yang menyebutkan bahwa musuh menyerang infrastruktur komersial (pelabuhan, logistik) yang diandalkan oleh suatu negara. Kemudian musuh yang menggunakan AI mengetahui hal tersebut dan mereka tidak perlu menyerang kapal perang negara tersebut, karena mereka hanya perlu menyerang *router* sipil atau *software* logistik komersial yang digunakan kapal perang untuk berkomunikasi. Analisis tantangan ROE adalah serangan terhadap *router* sipil atau sistem *Vessel Traffic Service* (VTS) telah memicu tantangan yurisdiksi. ROE militer tidak dapat melindungi infrastruktur sipil secara langsung, sehingga memungkinkan musuh menyerang celah di antara lembaga negara yang berkaitan dengan komunikasi maupun logistik.

Studi kasus kedua adalah *Lawfare* Hibrida yang melibatkan aktor non-negara, dimana secara fisik mereka bertujuan untuk menghambat proyek kabel data bawah laut di perairan internasional (ancaman ekonomi strategis) dan secara bersamaan melakukan *lawfare* (perang hukum) dengan menuduh staf PBB melakukan spionase (DPA International, 2025). Penggunaan ROE akan dihadapkan dengan pernyataan apakah ini terorisme, kejahatan transnasional, atau tindakan perang proksi, sedangkan ROE yang terfragmentasi pada kekuatan militer yang didukung dengan Kementerian/Lembaga negara akan gagal memberikan satu jawaban koheren.

Tantangan Proporsionalitas (Menyerang Respons Non-Kinetik)

ROE memiliki keunggulan dalam merespons ancaman kinetik, namun gagal total dalam merespons ancaman non-kinetik yang memiliki dampak strategis (Lee, 2023). Studi kasus yang terjadi menunjukkan peningkatan 800% insiden *spoofing* GNSS (Q2, 2025). Hal tersebut menandakan bahwa serangan non-kinetik yang dapat menyebabkan kerusakan fisik katastrofik (tabrakan tanker di alur pelayaran). Analisis tantangan pada ROE adalah apa respons proporsional terhadap *spoofing*, sedangkan ROE tidak memiliki opsi balasan yang terukur terhadap pelaku yang tidak terlihat. Kita tidak bisa meluncurkan rudal sebagai respons terhadap sinyal radio yang mengganggu.

"Kesenjangan Kecepatan" pada akhirnya menjadi tantangan proporsionalitas yang paling fundamental karena kecepatan adalah senjata. Analisis yang ada pada ROE menjawab bahwa terdapat proses yang lambat, manusiawi dan deliberatif. Namun kondisi yang berkembang saat ini adalah kehadiran AI sebagai musuh mampu beroperasi dengan siklus OODA dalam hitungan milidetik. Pada saat kita berhasil mengatribusikan serangan dan memutuskan respons yang proporsional, maka musuh (dengan siklus

iterasi mingguan) mungkin sudah mengubah vektor serangannya sebanyak tiga kali. Oleh karena itu, tidak berlebihan jika kita menjawab bahwa ROE yang lambat secara doktrinal *tidak proporsional* dengan *kecepatan* ancaman algoritmik (Payne, 2021).

D. PENUTUP

Dalam menghadapi ancaman modern, tantangan terkait atribut, proporsionalitas, dan yurisdiksi semakin kompleks. Pertama, tantangan atribusi muncul dari serangan rantai pasok dan siber yang mengaburkan identitas dan niat musuh, sehingga aturan keterlibatan (ROE) yang berbasis atribusi menjadi tidak relevan. Kedua, tantangan proporsionalitas ditimbulkan oleh serangan non-kinetik, seperti spoofing GNSS dan praktik lawfare, yang menciptakan dampak strategis yang setara dengan blokade, namun ROE saat ini tidak menawarkan opsi respons kinetik yang sah dan proporsional. Ketiga, tantangan yurisdiksi berpuncak pada serangan terhadap infrastruktur dual-use, di mana AI memanfaatkan celah antara yurisdiksi militer dan sipil. Kondisi ini mengharuskan kita untuk mendesain kembali kerangka regulasi dan strategi respons, agar dapat beradaptasi dengan dinamika ancaman yang berkembang cepat dan kompleks.

Sebagai kesimpulan, perlu ada perbaikan signifikan dalam aturan keterlibatan (ROE) dengan fokus pada efek daripada metode, untuk menjawab tantangan dari serangan non-kinetik yang dapat mengganggu infrastruktur kritis nasional. Setiap serangan terverifikasi harus secara otomatis dianggap sebagai Tindakan Bermusuhan, yang akan mengaktifkan protokol respons pertahanan tanpa mempedulikan identitas pelakunya. Selain itu, pembentukan Intel-Legal Fusion Cell sangat diperlukan untuk mengubah sistem peringatan dini menjadi penyedia keputusan yang cepat dan akurat, memberikan rekomendasi real-time terkait atribusi, status hukum, dan opsi respons hukum terhadap ancaman hibrida. Upaya ini tidak hanya mendorong efisiensi dalam pengambilan keputusan tetapi juga meningkatkan kolaborasi antara berbagai lembaga untuk mengatasi kompleksitas ancaman yang ada. Terakhir, akuntabilitas dan transparansi dalam tata kelola merupakan fondasi utama untuk membangun kepercayaan, yang pada gilirannya esensial untuk mencapai reformasi yang efektif. Tanpa adanya kepercayaan, inisiatif-inisiatif ini akan sulit dilaksanakan dan kurang mendapatkan dukungan. Oleh karena itu, membangun siklus pembelajaran doktrinal yang ideal menjadi prasyarat untuk meningkatkan kapasitas respons dan adaptasi terhadap dinamika ancaman yang terus berkembang. Langkah-langkah tersebut diharapkan dapat menciptakan kerangka kerja yang lebih responsif dan adaptif dalam era yang dipenuhi dengan ancaman hibrida.

D. DAFTAR PUSTAKA

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series.

Allen, G. C. (2024, Mei 10). *A Deep Dive into the US-China AI Rivalry and its Global Implications* [Video]. YouTube. https://www.youtube.com/watch?v=Lbk1WKFmIR0

Bleeping Computer. (2025, 30 Oktober). *Ex-L3Harris Executive Guilty of Selling Cyber Exploits to Russian Broker*. (Dikutip dari *Spy News, Week 44, 2025*).

Bueger, C. (2015). What is Maritime Security? *Marine Policy*, 53, 159–164.

Bueger, C., & Edmunds, T. (2017). Beyond seablindness: A new agenda for maritime security studies. *International Affairs*, 93(6), 1293–1311.

C3 AI. (2025, Mei 22). *AI-Powered Maritime Operations for Naval Fleet Readiness | C3 AI Federal Forum 2025* [Video]. YouTube. https://www.youtube.com/watch?v=sd_gWrP2FCg

CNBC Indonesia. (2021, 26 April). *Tragedi Nanggala, Connie Desak Audit Total Alutsista TNI!*. Diakses 9 November 2025, dari https://www.cnbcindonesia.com/news/20210426133829-4-240899/tragedi-nanggala-connie-desak-audit-total-alutsista-tni

Cole, R. (2025, Januari 17). *Transformational AI Adoption in the U.S. Navy: A Fireside Chat with the U.S. Navy and Domino* [Video]. YouTube. https://www.youtube.com/watch?v=gWgxvl3GAu8

Cullen, P. J., & Reichborn-Kjennerud, E. (2017). *Understanding Hybrid Warfare*. Oslo: Norwegian Institute of International Affairs.

Data Q2 2025. (2025). (Merujuk pada data hipotetis tentang *spoofing* GNSS yang digunakan dalam analisis naskah, didasarkan pada tren laporan industri maritim).

Detik News. (2025, 23 September). *KPK Panggil Eks Dirut PT DKB di Kasus Korupsi Kapal Angkut Tank TNI AL*. (Dirujuk secara kolektif sebagai Kompas, 2025).

DPA International. (2025, 31 Oktober). *Houthis Plan Espionage Trial for Detained UN Staff*. (Dikutip dari *Spy News, Week 44, 2025*).

DPR RI. (2020). *Kesiapan Alutsista TNI: Tinjauan atas Capaian MEF II (2015-2019) dan Tantangan MEF III (2020-2024)*. Jakarta: Pusat Kajian Anggaran DPR RI.

Haase, J. (2025, Maret 25). *AI, autonomy, and the future of naval warfare with Captain Jon Haase, United States Navy* [Video]. YouTube. https://www.youtube.com/watch?v=guxzPymyz-w

Heuser, B. (2010). *The Evolution of Strategy: Thinking War from Antiquity to the Present*. Cambridge, UK: Cambridge University Press.

Hoffman, F. G. (2009). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.

Horowitz, M. C. (2020). *The AI-Enabled Military: A Strategy for the Future*. Washington, D.C.: Center for a New American Security (CNAS).

Johnson, J. (2023). *Artificial Intelligence and the Future of Warfare*. Washington, D.C.: Georgetown University Press.

Johnson, R., & Li, X. (2024). Grey Zone Operations and International Law. *Journal of Strategic Studies*, 47(1), 1-25.

Jurnal Humaniora Revolusioner. (t.t.). *Sinergitas Bakamla dan TNI AL dalam Penegakan Hukum di Laut Natuna Utara*. (Dirujuk secara koleDktif sebagai Jurnal UPY, 2023).

Jurnal Maritim Indonesia. (2024). *Optimalisasi Operasi Bakamla RI Guna Mendukung Penegakan Hukum dan Keamanan Laut*. *Jurnal Maritim Indonesia*, 12(1).

Jurnal Syntax Imperatif. (2025). *Evaluasi Kebijakan Minimum Essential Force (MEF) 2010-2024*. (Dirujuk secara kolektif sebagai DPR RI, 2020).

Jurnal UPY. (2023). *Efektivitas Badan Keamanan Laut (Bakamla) dalam Penegakan Hukum di Zona Ekonomi Eksklusif Indonesia*. *Jurnal Ilmiah UPY*, 11(2).

Kania, E. B. (2017). *Maritime Militia and PLA Navy 'Grey Zone' Operations*. Washington, D.C.: Center for a New American Security (CNAS).

Kemenhan. (2023). *Rincian Alokasi Anggaran Belanja Kemenhan/TNI TA 2023*. Jakarta: Kementerian Pertahanan RI.

Kilcullen, D. (2020). *The Dragons and the Snakes: How the West Fought the Rest*. Oxford, UK: Oxford University Press.

Klein, N. (2021). Maritime Security and the Law of the Sea: The Challenge of Grey Zone Operations. *International Law Studies*, 97, 348-380.

Kompas. (2025, 23 September). *KPK Panggil Eks Dirut PT DKB Terkait Korupsi Pengadaan Kapal Angkut Tank TNI AL*. Diakses 9 November 2025, dari https://www.kompas.com/..

Kraska, J., & Pedrozo, R. (2013). *International Maritime Law*. Leiden: Martinus Nijhoff Publishers.

Kumparan. (2021, 28 April). *Pangkoarmada II: KRI Nanggala-402 Tak Punya Black Box, Investigasi Butuh Waktu*. Diakses 9 November 2025, dari https://kumparan.com/kumparannews/pangkoarmada-ii-kri-nanggala-402-tak-punya-black-box-investigasi-butuh-waktu-1vcL9eS4E9x

Lee, E. (2023). Proportionality in Cyber Warfare: A Failed Concept. *Texas International Law Journal*, 58(2), 201-230.

Maness, R. C., & Valeriano, B. (2018). The Impact of Attribution on Cyber Conflict. *Journal of Cybersecurity*, 4(1), 1-15.

Middle East Monitor. (2025, 30 Oktober). *Ex-Mossad Chief, Behind ICJ Blackmail Campaign, Brags Israel has Installed a Global Sabotage Network*. (Dikutip dari *Spy News, Week 44, 2025*).

Milne, R. (2025). *Shadow fleets, cyber-attacks, and spy ships*. The Guardian. (Dikutip dari *Spy News, Week 44, 2025*).

Morris, L. (2022). *Gaining Advantage in the Grey Zone*. Santa Monica, CA: RAND Corporation.

Payne, K. (2021). *I, Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst & Company.

Praja, A. S. I. (2024). Perkuatan Sistem Pertahanan Maritim Nusantara di Era Transformasi Digital. *Jurnal Maritim Indonesia*, 12(2), 54-63. http://doi.org/10.52307/jmi.v912.167

Putri, S.A & Burhanuddin, A.S (2023). "Maritime Cybersecurity: Tantangan Dan Strategi Keamanan Maritim Indonesia." *Mandub : Jurnal Politik, Sosial, Hukum Dan Humaniora 2*(1):378–86.

RAND Corporation. (2024). *The Strategic Implications of AI-Enabled Disinformation*. Santa Monica, CA: RAND Corporation.

Roberts, N., & Chen, Y. (2023). Decision-Making under Ambiguity: Cognitive Paralysis in Hybrid Warfare. *Security Studies*, 32(3), 401-430.

Roscini, M. (2020). *International Law and the Use of Force in the Cyber Age*. Oxford, UK: Oxford University Press.

Schmitt, M. N. (Ed.). (2019). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, UK: Cambridge University Press.

Sindo News. (2021, 23 April). *KSAL: KRI Nanggala-402 Tenggelam Bukan karena Human Error*. Diakses 9 November 2025, dari https://nasional.sindonews.com/read/308431/14/ksal-kri-nanggala-402-tenggelam-bukan-karena-human-error-1619179512

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. Boston, MA: Eamon Dolan/Houghton Mifflin Harcourt.

Smit, M. (2022). The Democratization of AI in Hybrid Warfare. *Journal of Information Warfare*, 21(2), 70-85.

Strobel, W. (2025). *NATO steps up undersea infrastructure defense*. The Wall Street Journal. (Dikutip dari *Spy News, Week 44, 2025*).

Talpur, K., et al. (2025). AI in Maritime Security: Applications, Challenges, Future Directions, and Key Data Sources. *Information*, 16(8), 658.

The Record. (2025, 31 Oktober). *Chinese Hackers Scanning, Exploiting Cisco ASA Firewalls Used by Governments Worldwide*. (Dikutip dari *Spy News, Week 44, 2025*).

UNCTAD. (2023). *Review of Maritime Transport 2023*. Geneva: United Nations Conference on Trade and Development.

United Nations. (1982). *United Nations Convention on the Law of the Sea (UNCLOS)*. Montego Bay.

Wikipedia. (2025, 22 Juli). *Jalesveva Jayamahe*. Diakses 9 November 2025, dari https://id.wikipedia.org/wiki/Jalesveva_Jayamahe

Wirtz, J. J. (2021). The Grey Zone Challenge to Deterrence. *Journal of Strategic Security*, 14(3), 1-14.