

Bibliography

Books

Ashworth, Andrew, and Lucia Zedner. *Preventive Justice*. Oxford: Oxford University Press, 2014.

Brenner, Susan W. *Cybercrime: Criminal Threats from Cyberspace*. University of Dayton School of Law Faculty Publications, 2010.
https://ecommons.udayton.edu/law_fac_pub/115.

Efendi, Jonaedi, and Johnny Ibrahim. *Metode Penelitian Hukum Normatif dan Empiris*. Edisi 1. Jakarta: Kencana, 2016.

Findlay, Mark, et al. *Australian Criminal Justice*. 5th ed. South Melbourne, VIC: Oxford University Press, 2014.

Gargiulo, Pietro, Davide Giovannelli, and Annita Larissa Sciacovelli, eds. *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*. Napoli: Editoriale Scientifica, 2024.

Klopper, Franziska, ed. *Accountability in Cybersecurity*. Geneva: Geneva Centre for Security Sector Governance, 2024.

Laidlaw, Gregory, and Charles E. Wilson. *Cyber Criminology, Criminology and Cybercrime: Towards an Academic Discipline*. University of Detroit Mercy, Center for Cyber Security and Intelligence Studies, n.d.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2017.

Roberts, Anthea. *Risk, Reward, and Resilience*. Canberra: School of Regulation and Global Governance (RegNet), Australian National University, 2022. <https://regnet.anu.edu.au>.

Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: UI Press, 2010.

Solmaz, M.S., et al. "Digital Transformation in Port Management: Smart Ports." In *Managerial Issues in Digital Transformation of Global Modern Corporations*. IGI Global, 2019.

Wiradipradja, E. Saefullah. *Penuntun Praktis Metode Penelitian dan Penulisan Karya Ilmiah Hukum*. Bandung: Keni Media, 2015.

Journal

Akpan, Frank, et al. "Cybersecurity Challenges in the Maritime Sector." *Network 2* (2022): 123–138.

Alanazi, Manar, et al. "SCADA Vulnerabilities and Attacks: A Review of the State-of-the-Art and Open Issues." *Computers & Security* 125 (2023): 103028. <https://doi.org/10.1016/j.cose.2022.103028>.

Aldino, Hanri et al. "The Role of Criminal Law in Enforcing Good Corporate Governance as an Instrument for Strengthening Business Integrity in Indonesia." *Samudra Justicia Law Journal* 1, no. 1 (December 2025): 13.

Alfian, et al. "Revolusi Digital Maritim: Analisis Yuridis Keamanan Siber di Pelabuhan dan Kekuatan Pembuktian Electronic Bill of Lading." *Journal of Innovative and Creativity* 5, no. 3 (2025).

Almalawi, Abdulmohsen, et al. "Hybrid Cybersecurity for Asymmetric Threats: Intrusion Detection and SCADA System Protection Innovations." *Symmetry* 17, no. 4 (April 2025): 616. <https://doi.org/10.3390/sym17040616>.

Alpajri, Muhammad, Erdianto, and Davit Rahmadan. "Strengthening Indonesia's EIT Law to Combat Ransomware Threats: A Legal Framework Analysis." *Jurnal Ilmiah Advokasi* 13, no. 2 (July 2025): 403.

Androjna, Andrej, Tanja Brcko, Ivica Pavić, and Harm Greidanus. "Assessing Cyber Challenges of Maritime Navigation." *Journal of Marine Science and Engineering* 8, no. 10 (2020).

Arimbhi, Pebriana, et al. "Implementation of the National Logistic Ecosystem Program in Increasing the Performance of the National Logistics System, Improving the Investment Climate, and Increasing the Competitiveness of the National Economy." *Budapest International Research and Critics Institute (BIRCI) Journal* 4, no. 4 (2021): 9054–9066. <https://doi.org/10.33258/birci.v4i4.2673>.

Banakar, Reza. "Law through Sociology's Looking Glass." *International Journal of Law in Context* 2, no. 1 (2006): 61–68.

Benmalek, Mourad. "Ransomware on Cyber-Physical Systems." *Internet of Things and Cyber-Physical Systems* 4 (2024): 186–202. <https://doi.org/10.1016/j.iotcps.2024.04.002>.

Bueger, Christian. "A Glue That Withstands Heat? The Promise and Perils of Maritime Domain Awareness." In *Maritime Security: Counter-Terrorism Lessons from Maritime Piracy and Narcotics Interdiction*, edited by E. R. Lucas et

al., 235–248. Amsterdam: IOS Press, 2020.

<https://doi.org/10.3233/NHSDP200065>.

Bueger, Christian, and Tobias Liebetrau. “Critical Maritime Infrastructure Protection.” *Marine Policy* 155 (2023): 105772.

<https://doi.org/10.1016/j.marpol.2023.105772>.

Busetti, Simone, and Francesco Maria Scanni. “Evaluating Incident Reporting in Cybersecurity.” *Government Information Quarterly* 42 (2025): 102000. <https://doi.org/10.1016/j.giq.2024.102000>.

Daukere, Bitrus Eniyekenimi, and Ifatokun Paul Ifabiyi. “Socio-Environmental Factors and Organized Criminal Networks Influencing Maritime Crime Dynamics in Nigeria’s Niger Delta.” *Environmental Challenges* 20 (2025): 101263. <https://doi.org/10.1016/j.envc.2025.101263>.

De Faria, Duarte Lynce. “The Impact of Cybersecurity on the Regulatory Legal Framework for Maritime Security.” *Janus.net: e-Journal of International Relations* 11, no. 2 (November 2020–April 2021): 164. <https://doi.org/10.26619/1647-7251.11.2.10>.

Desiana, Rizki, and Sri Cempaka Prima. “Cyber Security Policy in Indonesian Shipping Safety.” *Journal of Maritime Studies and National Integration* 5, no. 2 (2022): 110. <https://doi.org/10.14710/jmsni.v5i2.13673>.

Djajasinga, Nico Djundharto, et al. “Risk Management in the Digital Era: Addressing Cybersecurity Challenges in Business.” *Branding: Jurnal Ilmiah Manajemen dan Bisnis* 26 (2023): 29–38. <https://www.journal.uinsgd.ac.id/index.php/branding>.

Durlik, Irmina, et al. *Navigating the Sea of Data: A Comprehensive Review on Data Analysis in Maritime IoT Applications*. *Applied Sciences* 13, no. 19 (2023): 9742.

Egloff, Florian J. "Contested Public Attributions of Cyber Incidents." *Contemporary Security Policy* 41, no. 1 (2019): 55–81.
<https://doi.org/10.1080/13523260.2019.1677324>.

Erbas, Muhammed, et al. "Systematic Literature Review of Threat Modeling." *Ocean Engineering* 306 (2024): 118059.
<https://doi.org/10.1016/j.oceaneng.2024.118059>

Faisal, Ahmad, et al. "Cybersecurity in Digital Supply Chains: A Narrative Review of Threats and Strategic Frameworks for Sustainable Logistics." *Sinergi International Journal of Logistics* 2, no. 3 (2024): 177.

Farah, Ben & Mohamed Amine, et al. "Cyber Security in the Maritime Industry A Systematic Survey of Recent Advances and Future Trends." *Information* 13, no. 1 (2022): 22. <https://doi.org/10.3390/info13010022>

Firdani, Arief Nashrul, and Heri Supomo. "Analysis of Constraints in Implementing Inaportnet at Sorong Port Class 1." *International Journal of Offshore and Coastal Engineering* 8, no. 1 (2024): 53–58.

Greiman, V. A. "Defending the Cyber Sea: Legal Challenges Ahead." *Journal of Information Warfare* 19, no. 3 (2020): 68–82.
<https://www.jstor.org/stable/10.2307/27033633>.

Gunasekaran, Periasamy. "Malaysian Port Security: Issues and Challenges." *Australian Journal of Maritime & Ocean Affairs* (2012).
<https://doi.org/10.1080/18366503.2012.10815702>.

Harish, Avanthika Vineetha, et al. "Literature Review of Maritime Cyber Security: The First Decade." *Maritime Technology and Research* 7, no. 2 (2025).
<https://doi.org/10.33175/mtr.2025.273805>.

Hashmi, Muhammad Ahsan Iqbal, et al. "Cybercrime and Digital Offenses: Challenges of Applying Traditional Criminal Law." *Journal of Social & Organizational Matters* 4, no. 4 (2025): 256.
<https://doi.org/10.56976/jsom.v4i4.343>.

Hasnia, et al. "Reconstruction of Criminal Law Policy in Handling Cyber Crime: Perspectives of Technology Law and Human Rights." *Jurnal Smart Hukum* 3, no. 3 (2025): 254. <https://doi.org/10.55299/jsh.v3i3.1328>.

Hoffmann, Romuald, et al. "Risk-Based Approach in Scope of Cybersecurity Threats and Requirements." *Procedia Manufacturing* 44 (2020): 656–661. <https://doi.org/10.1016/j.promfg.2020.02.243>.

Hutchinson, Terry. "Doctrinal Research: Researching the Jury." *Journal of Law and Society* 36, no. 1 (2009): 103–109.

Idris, Muhammad, et al. "Analysis of the Inaportnet System That Affects the Ship Service of PT Kartika Samudra Adijaya at the Port of Samarinda." *Asian Journal of Social and Humanities* 2, no. 1 (March 6, 2024).

Iswanto, et al. "Efforts to Reduce Gaps in System and Procedure Irregularities at Ports." *International Journal of Economics, Business and*



Innovation Research (IJEBIR) 2, no. 2 (2023). <https://e-journal.citakonsultindo.or.id/index.php/IJEBIR>.

Jin, Yongming, et al. “Navigating the Digital Seas: Legal Challenges and Global Governance of Maritime Cyber Operations.” *Frontiers in Marine Science* 12 (2025): 1616906. <https://doi.org/10.3389/fmars.2025.1616906>.

Jr., Joseph S. Nye, “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (Winter 2016/17): 44–71. https://doi.org/10.1162/ISEC_a_00266.

Kapalidis, Chronis, Stavros Karamperidis, Tim Watson, and Georgios Koligiannis. “A Vulnerability-Centric System-of-Systems Analysis on the Maritime Transportation Sector’s Most Valuable Assets: Recommendations for Port Facilities and Ships.” *Journal of Marine Science and Engineering* 10 (2022): 1486.

Karim, Md Saiful. “Maritime Cybersecurity and the IMO Legal Instruments.” *Marine Policy* 143 (2022): 105138. <https://doi.org/10.1016/j.marpol.2022.105138>.

Keskin, Omer F. “Systematic Cyber Threat Modeling for Maritime Operations: Attack Trees for Shipboard Systems.” *WMU Journal of Maritime Affairs* 22, no. 2 (2023): 267–296. <https://doi.org/10.1007/s13437-023-00290-8>.

Lee, Young-Chan, et al. “Improving Cyber Security Awareness in Maritime Transport: A Way Forward.” *Journal of the Korean Society of Marine Engineering* 41, no. 8 (2017): 738.

Li, Meixuan, Jianying Zhou, Sudipta Chattopadhyay, and Mark Goh. "Maritime Cybersecurity: A Comprehensive Review." *IEEE Transactions on Intelligent Transportation Systems* (2024).

Li, Yuchong, and Qinghui Liu. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments." *Energy Reports* 7 (2021): 8176–8186.

Liu, Gaiyun, et al. . "Survey and Future Trends for Cybersecurity in Maritime and Port Sectors: A Discrete Event Systems Perspective." *Mathematics* 13, no. 22 (2025): 3650. <https://doi.org/10.3390/math13223650>.

Marchiafava, Giovanni. "Cybercrime and Cybersecurity in Shipping: A Legal Framework in Progress." *Rivista di Studi Politici Internazionali* 89, no. 2 (2022): 239–258. <https://www.jstor.org/stable/10.2307/27273621>.

Melander, Sakari. "Preventive Turn in Criminal Law." *Peking University Law Journal* 11, no. 1 (2023): 13. <https://doi.org/10.1080/20517483.2023.2223843>.

Mizrak, Filiz. "Integrating Cybersecurity Risk Management into Strategic Management: A Comprehensive Literature Review." *Research Journal of Business and Management* 10, no. 3 (2023): 101–110. <https://doi.org/10.17261/Pressacademia.2023.1807>.

Mohsendokht, Massoud, et al. "Decoding Dependencies among the Risk Factors Influencing Maritime Cybersecurity: Lessons Learned from Historical Incidents in the Past Two Decades." *Ocean Engineering* 312 (2024): 119078.

Mufidasari, Asmaul, Amarulla Octavian, and Herlina Juni Risma Saragih. “Implementasi Sistem Pengamanan Informasi dalam Aplikasi Inaportnet untuk Maritime Cyber Security.” *Jurnal Keamanan Maritim* 5, no. 1 (2019): 1–12.

Mukherjee, Proshanto K. “The ISM Code and the ISPS Code: A Critical Legal Analysis of Two SOLAS Regimes.” *WMU Journal of Maritime Affairs* 6, no. 2 (2007): 147–166.

Nagin, Daniel S., et al. “Deterrence in the Twenty-First Century.” *Crime and Justice* 42, no. 1 (2013): 1–63. <https://doi.org/10.1086/670398>.

Nimmich, Joseph L., and Dana A. Goward. “Maritime Domain Awareness: The Key to Maritime Security.” In *Global Legal Challenges: Command of the Commons, Strategic Communications, and Natural Disasters*, edited by Michael D. Carsten, vol. 83, *International Law Studies*. Newport, RI: United States Naval War College. Accessed November 16, 2024. <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1160&context=ils>.

Nimot, Senitriany Beatrix, et al. “Analysis of the Effectiveness of Inaportnet in Supporting Ship Document Services at Soekarno-Hatta Port.” *International Journal of Engineering Trends and Technology* 72, no. 10 (2024): 352–356. <https://doi.org/10.14445/22315381/IJETT-V72I10P134>.

Nissa, Khaoeirun. “From ‘Criminal Acts’ to ‘Crimes’ and Accountability: A Philosophical Study of the Aspects of Fault and Punishment in Law No. 1 of 2023.” *Jurnal Legislasi dan Penegakan Hukum* 6, no. 1 (2025): 328. <https://doi.org/10.38035/jlph.v6i1>.

Novia, Betti. “Legal Responsibility for Perpetrators of Criminal Acts of Assault (Study of Decision Number 5/Pid.B/2025/Pn Tpg).” *Ratio Legis Journal* 4, no. 4 (December 2025): 3188.

Onyemechi, Chinedum. “Improving West Africa’s Coastal Security Management: An Analytical Model.” *Journal of Coastal Zone Management* (2016). <https://doi.org/10.4172/2473-3350.1000429>.

Panteli, Niki, Boineelo R. Nthubu, and Konstantinos Mersinas. “Being Responsible in Cybersecurity: A Multi-Layered Perspective.” *Information Systems Frontiers* (2025). <https://doi.org/10.1007/s10796-025-10588-0>.

Patterson, Clare M., et al. “Learning from Cyber Security Incidents: A Systematic Review and Future Research Agenda.” *Computers & Security* 132 (2023): 103309. <https://doi.org/10.1016/j.cose.2023.103309>.

Peno, Michał. “The Character of the Principles of Criminal Law and Criminal Responsibility: Between the Philosophy of Law and Semiotic.” *Liverpool Law Review* 40 (2019): 80. <https://doi.org/10.1007/s10991-019-09226-y>.

Pifferi, Michele. “Criminal Responsibility and Its Histories: New Perspectives for Comparative Legal History.” *Critical Analysis of Law* 4, no. 2 (2017): 225. <https://cal.library.utoronto.ca/index.php/cal/article/view/30765>.

Pool, Javad, et al. “A Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review.” *International Journal of Information Management* 74 (2024): 102719. <https://doi.org/10.1016/j.ijinfomgt.2023.102719>.

Prasad, Nilantha, et al. "A Survey of Cyber Threat Attribution: Challenges, Techniques, and Future Directions." *Computers & Security* 157 (2025): 104606. <https://doi.org/10.1016/j.cose.2025.104606>.

Pseftelis, Thanasis, and Gregory Chondrokoukis. "A Study about the Role of the Human Factor in Maritime Cybersecurity," *SPOUDAI: Journal of Economics and Business* 71, no. 1–2 (2021): 55–72. <https://hdl.handle.net/10419/283673>.

Raskolnikov, Alex. "Deterrence Theory: Key Findings and Challenges." In *The Cambridge Handbook of Compliance*. Cambridge: Cambridge University Press, 2021. <https://doi.org/10.1017/9781108759458.014>.

Riadi, Bintang Rahmat, et al. "Risk Management of Information Security in Inaportnet Using ISO/IEC 27005:2018." *Jurnal Inovtek Polbeng-Seri Informatika* 10, no. 1 (2025): 225–236.

Rizaldy, Robby, Satriya Wibawa, and Arfin Sudirman. "Cybersecurity Challenges in the Malacca Straits: Indonesia's Strategic Approach Through BSSN and IMIC." *Jurnal Wacana Politik* 10, no. 2 (2025): 243–244. <https://doi.org/10.24198/jwp.v10i2.57343>.

Rusman, and Ahmad Kamaludin. "Investigation of Cyber Crime in the Indonesian Legal Framework." *Journal La Sociale* 5, no. 6 (2024): 1576. <https://doi.org/10.37899/journal-la-sociale.v5i6.1367>.

Saipudin, Lalu, et al. "The Concept of Corporate Criminal Liability in the Indonesian Criminal Law System." *Jurnal IUS Kajian Hukum dan Keadilan* 13, no. 2 (August 2025): 477. <https://doi.org/10.29303/ius.v13i2.1817>.

Sangari, Seema, et al. "Modeling Under-Reporting in Cyber Incidents." *Risks* 10, no. 11 (2022): 200. <https://doi.org/10.3390/risks10110200>.

Sasi, Tinshu, et al. "A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges." *Journal of Information and Intelligence* 2 (2024): 456. <https://doi.org/10.1016/j.jiixd.2023.12.001>.

Schwarz, Monina, Matthias Marx, and Hannes Federrath. "A Structured Analysis of Information Security Incidents in the Maritime Sector." *arXiv* (2021)

Senarak, Chalermpong. "Leveraging Advanced Technologies and Strategies for Port Cyber Resilience: Strengthening Incident Response and Recovery." *Transportation Research Interdisciplinary Perspectives* 34 (2025): 101666. <https://doi.org/10.1016/j.trip.2025.101666>.

Sianturi, Putra Sanjaya, and Fadiyah Hani Sabila. "The Influence of Manual System Port Services to Inaportnet on Users of Belawan Port Services at PT Adhigana Pratama Mulya Belawan." *Jurnal Pajak dan Analisis Ekonomi Syariah* 1, no. 1 (2024): 17–27. <https://doi.org/10.61132/jpaes.v1i1.198>.

Sonitioso, Yos. "Port Performance Factors and Their Interactions: A Systems Thinking Approach." *Research in Transportation Business & Management* 50 (2024): 101057. <https://doi.org/10.1016/j.rtbm.2024.101057>.

Sulubara, Seri Mughni, et al. "Legal Protection of Cybercrime Crimes from Ransomware Attacks and Evaluation of the Cyber Security and Resilience Bill 2025 in Indonesia's Defense." *De Lega Lata: Jurnal Ilmu Hukum* 10, no. 2 (July–December 2025): 288. <https://doi.org/10.30596/dll.v10i2.25786>.

Syifa, Given Abi, and Muhammad Tohir. "Analysis of Logistics Cost Efficiency in Indonesia's Transportation System." *Siber Journal of Transportation and Logistic* 3, no. 2 (July–September 2025): 45–56.

Tetley, William. "Mixed Jurisdictions: Common Law vs. Civil Law." *Louisiana Law Review* 60, no. 3 (2000): 677–738.

Thai, Vinh V., and Devinder Grewal. "The Maritime Security Management System: Perceptions of the International Shipping Community." *Maritime Economics & Logistics* (2007). <https://doi.org/10.1057/palgrave.mel.9100175>.

Tijan, Edvard, et al. "Digital Transformation in the Maritime Transport Sector." *Technological Forecasting and Social Change* 170 (2021): 120879. <https://doi.org/10.1016/j.techfore.2021.120879>.

Todorov, Yavor. "Maritime Cyber(in)security: A Growing Threat Imperils EU Countries." *Connections: The Quarterly Journal* 20, nos. 3–4 (2021): 73–93.

Utama, Dani Rusli, et al. "Developing a Digital Transformation Maturity Model for Port Assessment in Archipelago Countries: The Indonesian Case." *Transportation Research Interdisciplinary Perspectives* 26 (2024): 101146.

Verma, Ritesh. "Cybersecurity Challenges in the Era of Digital Transformation." In *Recent Advances in Computer Science and Information Technology*, edited by R. K. Sharma. New Delhi: Bharati Publications, 2023. <https://doi.org/10.25215/9392917848.20>.

William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010): 99.

Wilmsmeier, Gordon, et al. "Port Governance and the Implications of Institutional Fragmentation: Lessons from Colombia." *Research in Transportation Business & Management* 56 (2024): 101179. <https://doi.org/10.1016/j.rtbm.2024.101179>.

Xu, Yuanyuan, et al. "A Multidisciplinary Review into the Evolution of Risk Concepts and Their Assessment Methods." *Reliability Engineering & System Safety* 217 (2022): 108063. <https://doi.org/10.1016/j.res.2021.108063>.

Reports & Working Paper

Department of the Navy, United States. *Report on the Collision Between USS Lake Champlain and a Fishing Vessel in the Pacific Ocean, May 2017*. Memorandum of Distribution. Washington, DC: Department of the Navy, 2017.

Dragos Inc. *Industrial Ransomware Attack Analysis: Q2 2023*. August 2023.

European Union Agency for Cybersecurity (ENISA). *Cybersecurity for Ports and Port Systems*. 2019.

European Union Agency for Cybersecurity (ENISA). *ENISA Transport Threat Landscape*. ENISA Reports, March 21, 2023. Accessed September 2, 2025. <https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape>.

Ewansiha, Favour Iyobosa, et al. *Enhancing Cyber Resilience in Ports: A Study of Cyber Threats and Response Systems in Ports*. Innovative Research Project, INP IAE, University of Grenoble Alpes, n.d.

Federal Aviation Administration. *Aviation Instructor's Handbook*, FAA-H-8083-9B. Updated 2020.



https://www.faa.gov/sites/faa.gov/files/regulations_policies/handbooks_manuals/aviation/aviation_instructors_handbook/03_aih_chapter_1.pdf.

Felsen-Parsons, Brit, Sarah Fu, Kirara Nakamura, and Schoni Song. *Improving and Operationalizing Maritime Domain Awareness in the South China Sea*. New York: Columbia University School of International and Public Affairs, May 2020.

International Chamber of Commerce (ICC). *Protecting the Cybersecurity of Critical Infrastructures and Their Supply Chains*. Working paper. 2024. Accessed March 4, 2025. https://docs-library.unoda.org/Opened_Working_Group_on_Information_and_Communication_Technologies_-_2021/ICC-2024_Protecting-the-cybersecurity-of-critical-infrastructures-and-their-supply-chains.pdf.

Johnson, Ben. *Do Criminal Laws Deter Crime? Deterrence Theory in Criminal Justice Policy: A Primer*. St. Paul, MN: Minnesota House Research Department, January 2019.

Meland, Phil H., et al. "A Retrospective Analysis of Maritime Cyber Security Incidents." 2021.

PT Integrasi Logistik Cipta Solusi (ILCS). *Digital Port Integrator: Laporan Tahunan 2023*. Jakarta: PT ILCS, 2024.

Standards Australia and Standards New Zealand. *AS/NZS 31000:2009 Risk Management—Principles and Guidelines*. Sydney/Wellington: Standards Australia/Standards New Zealand, 2009. https://www.isa.org.jm/wp-content/uploads/2022/12/asnzs_31000_2009.pdf.

The Institution of Engineering and Technology. *Good Practice Guide: Cyber Security for Ports and Port Systems*. London: IET, 2022.

Thompson, Madeleine, and Trey Herr. *The NotPetya Cyberattack: A Case Study for Understanding the Legal and Policy Challenges of Deterrence*. New York: Columbia University School of International and Public Affairs, 2022.
<https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf>.

United States Department of Homeland Security. *National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security*. Accessed November 16, 2024.
https://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf.

White House. *The Cost of Malicious Cyber Activity to the U.S. Economy*. Washington, DC: Executive Office of the President of the United States, 2018.
<https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>.

World Economic Forum. "Wild Wide Web—Consequences of Digital Fragmentation." In *The Global Risks Report 2020*, 15th ed., January 2020. Accessed June 20, 2020. <https://www.weforum.org/reports/the-global-risks-report-2020>

National Law

Law Number 7 2008 on Electronic Information and Transaction

Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016.



Law Number 17 2008 on Shipping

Law Number 32 of 2014 on Maritime Affairs

Government Regulation Number 5 of 2010 on Navigation

Government Regulation Number 31 of 2021 on the Implementation of the
Shipping Sector

Government Regulation Number 61 of 2009 on Ports Affairs

Government Regulation No. 71 of 2019 on the Operation of Electronic
Systems and Transactions

Government Regulation Number 101 of 2021 on Risk-Based Business
Licensing

Presidential Regulation Number 10 of 2008 on the Use of Electronic
Systems in Port Services

Presidential Regulation Number 28 of 2021 on SPBE (Electronic-Based
Government System) Architecture

Presidential Regulation Number 53 of 2017 on National Maritime Security

Presidential Regulation Number 47 of 2023 on National Cybersecurity
Strategy

Presidential Regulation Number 178 of 2014 on the Maritime Security
Agency (Bakamla)

Minister of Transportation Regulation Number PM 51 of 2015 on the
Organisation of Sea Ports

Minister of Transportation Regulation Number PM 157 of 2015 on The implementation of the Inaportnet system for ship and cargo services at Indonesian ports

Minister of Transportation Regulation Number PM 134 of 2016 on Standards and operational procedures for port services

Minister of Transportation Regulation Number PM 8 of 2022 on The centralized national implementation of the Inaportnet system

Ministerial Decree Number 33 of 2003 on the Implementation of SOLAS 1974

Bakamla Regulation Number 17 of 2021 on Coordination mechanisms for maritime security and safety operations in Indonesian waters

Bakamla Regulation Number 27 of 2021 on The organization and operation of maritime security surveillance and information systems

International Law

International Maritime Organization (IMO). *International Safety Management (ISM) Code*. Accessed February 27, 2025.

International Maritime Organization (IMO). *Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems*. Adopted June 16, 2017.

[https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428\(98\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf).

Legal Documents

Baltic and International Maritime Council (BIMCO), et al. *The Guidelines on Cyber Security Onboard Ships*. Version 4. London: BIMCO, 2021.

Council of Europe, *Explanatory Report to the Convention on Cybercrime*, European Treaty Series No. 185 (Budapest: Council of Europe, 2001).

European Commission and European Maritime Safety Agency (EMSA). *Guidance on How to Address Cybersecurity Onboard Ships During Audits, Controls, Verifications and Inspections (MARSEC Doc. 9209)*. Brussels: European Commission, November 8, 2023.

International Association of Ports and Harbors (IAPH). *Cybersecurity Guidelines for Ports and Port Facilities*. Version 1.0. Tokyo: IAPH, July 2, 2021.

International Maritime Organization (IMO). *Cyber Security*. Accessed February 27, 2025.

International Maritime Organization. *Guidelines on Cyber Security Onboard Ships*. Version 4. London: Collaboration between BIMCO, ICS, INTERCARGO, INTERTANKO, and IUMI, 2020.

International Maritime Organization (IMO). *Guidelines on Maritime Cyber Risk Management*. MSC-FAL.1/Circ.3/Rev.2, June 7, 2022.

Thesis & Dissertation

Aiken, Deniece. *Maritime Governance: Contextual Factors Affecting Implementation of IMO Instruments*. PhD diss., World Maritime University, 2023.

Erba, Alessandro. *Security Aspects of Anomaly Detection for Cyber-Physical Systems*. PhD diss., Saarland University, 2023.

Hulme, Marcus. *Preventive Justice: Law, Theory and Practice*. MPhil thesis, University of York, 2018.

Laksmiana, Teddy. *Cybersecurity in the Indonesian Maritime Sector: Challenges and Policy Implications*. PhD diss., Victoria University, 2022.

Official Websites

Atlassian. "RACI Chart: Roles and Responsibilities Explained." 2025. Accessed August 28, 2025. <https://www.atlassian.com/work-management/project-management/raci-chart>.

Bureau Veritas Marine & Offshore. "Marine Cybersecurity." <https://marine-offshore.bureauveritas.com/marine/cybersecurity>.

DNV. "Maritime Cyber Security Regulations." Accessed August 10, 2025. <https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/regulations/>.

European Commission. "Cyber Resilience Act: Reporting Requirements." *Digital Strategy*. Accessed February 7, 2026. <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>.

Kementerian Perhubungan Republik Indonesia. "Peningkatan Layanan Logistik Transportasi Laut Melalui Inaportnet Perlu Ditingkatkan." July 11, 2023.

Ministry of Transportation of the Republic of Indonesia. "Sistem Informasi Inaportnet." <https://portal.dephub.go.id/post/read/sistem-informasi-inaportnet>.



New Jersey Cybersecurity & Communications Integration Cell (NJCCIC).
“Maritime.” *Cybersecurity for Critical Infrastructure*. Accessed November 16,
2024. <https://www.cyber.nj.gov/threat-landscape/cybersecurity-for-critical-infrastructure/maritime>.

The Institution of Engineering and Technology (IET). *Good Practice of Cyber Security and Port System*. London: IET, 2022.
<https://www.theiet.org/media/12055/good-practice-guide-cybersecurity-port-system.pdf>.

United Nations Office on Drugs and Crime (UNODC). “Obstacles to Cybercrime Investigations.” In *Module 5: Key Issues in Cybercrime*. UNODC e-Learning. <https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html>.

United States Coast Guard (USCG). “Cyber Threats to Watch Out for in the Marine Transportation System.” *MyCG*, October 13, 2025. Accessed November 17, 2025. <https://www.mycg.uscg.mil/News/Article/3744151/cyber-threats-to-watch-out-for-in-the-marine-transportation-system/>.

Windward. “Maritime Domain Awareness.” Accessed November 16, 2024.
<https://windward.ai/glossary/what-is-maritime-domain-awareness/>.

News & Media

Al Jazeera. “Israel Cyberattack Caused ‘Total Disarray’ at Iran Port: Report.” *Al Jazeera*, May 19, 2020. Accessed November 16, 2024.
<https://www.aljazeera.com/news/2020/5/19/israel-cyberattack-caused-total->



[disarray-at-iran-port-report](#)

Coble, Sarah. "MSC Suffers Suspected Cyberattack." *Infosecurity Magazine*. Accessed November 16, 2024. <https://www.infosecurity-magazine.com/news/msc-suffers-suspected-cyberattack/>.

Fahim, Kareem, and Rick Gladstone. "Tankers Are Attacked in Mideast Gulf Region, and U.S. Says Video Shows Iran Was Involved." *The New York Times*, June 13, 2019. <https://www.nytimes.com/2019/06/13/world/middleeast/oil-tanker-attack-gulf-oman.html>.

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, August 22, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

Heimdahl Security. "HMM Reveals It Had Suffered a Cyberattack on Its Email Servers." Accessed November 16, 2024. <https://heimdalsecurity.com/blog/hmm-reveals-it-had-suffered-a-cyberattack-on-its-email-servers/>

Iyama, Noriyuki, and Junko Ogura. "Japan's Largest Port Hit by Ransomware Attack, Halting Operations." *CNN*, July 6, 2023. <https://edition.cnn.com/2023/07/06/tech/japan-port-ransomware-attack>.

"Maritime Industry Must Open Up about Cyber Crime." *Lloyd's List*, August 12, 2019.

Marks, Paul. "Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon." *New Scientist*, August 10, 2017. Accessed November 17, 2024.



<https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/>.

MaritimNews. “Perdana, Kemenhub Gelar Joint Exercise Port Facilities Cyber Attack & Traffic Impact.” February 29, 2024.

Nakashima, Ellen. “China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare.” *The Washington Post*, June 8, 2018. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

Reuters. “Exclusive: South Africa’s Transnet Hit by Cyber Attack – Sources.” *Reuters*, July 22, 2021. <https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/>.

Reuters. “Marine Firm James Fisher Reports Cyber Breach.” *Reuters*, November 5, 2019. <https://www.reuters.com/article/technology/marine-firm-james-fisher-reports-cyber-breach-idUSKBN1XF1SQ/>

Rizika, Robert. “Cyber Attacks on Maritime OT Systems Increased 900% in Last Three Years.” *SAFETY4SEA*, January 13, 2020. <https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/>

Sguazzin, Antony. “South Africa Port Operator Declares Force Majeure over Cyberattack.” *Bloomberg*, July 27, 2021.

Tempo.co. “Kemenhub: Sektor Maritim RI Rawan Kena Serangan Siber.” *Tempo.co*, March 13, 2024.

The Japan Times. “Japan Eyes Cybersecurity Improvements after Major Port Hit by Ransomware Attack.” *The Japan Times*, July 13, 2023.

The Record by Recorded Future. “Indonesia Holds Maritime Cybersecurity Exercise with the United States.” *The Record*, June 14, 2023.

USNI News. “U.S. Cruiser USS Lake Champlain Collides with South Korean Fishing Vessel.” May 9, 2017. <https://news.usni.org/2017/05/09/cruiser>.

Yudhi, Anastasya Lavenia. “Indonesia’s Maritime Sector Remains Vulnerable to Cyberattacks, Ministry Says.” *Tempo.co (English)*, September 5, 2025.

Internet

“Inaportnet Kunci Utama Pelabuhan di Indonesia Mampu Bersaing Secara Global.” *Mimbarmaritim.com*, October 24, 2024.

“Maritime Cybersecurity: Navigating the Challenges and Implementing Solutions.” *VirtueMarine*, January 2, 2025.

“Port Governance Models: Landlord, Tool, and Service Ports Explained.” *London Maritime Academy (lmitac.com)*, October 11, 2025. Accessed September 5, 2025. <https://www.lmitac.com/articles/landlord-tool-service-port-governance>.

AVS Global Supply. “What Is IMO? A Technical Guide for Maritime Operations.” April 21, 2025. <https://www.avsglobalsupply.com/blog-detail/imo>.

Babasaheb Bhimrao Ambedkar University. *Cyber Crimes and Laws*. Accessed March 22, 2025. <https://www.bbau.ac.in/dept/Law/TM/1.pdf>.

Baskoro, Aryo. “Permenhub 8/2022: Inaportnet as a Centralized System for Ship Services in Port.” *ARMA Law Newsflash*, April 28, 2022.

Boyes, Hugh, Roy Isbell, and Alexandra Luck. *Cyber Security for Ports and Port Systems: Good Practice Guide*. London: Institution of Engineering and Technology, 2020.

Graves, Jamie. “Reactive vs. Proactive Cybersecurity: 5 Reasons Why Traditional Security Strategies Fall Short.” *Fortinet Blog*, February 22, 2019. <https://www.fortinet.com/blog/industry-trends/reactive-vs--proactive-cybersecurity--5-reasons-why-traditional->

Kudo, Yasushi. *Cybersecurity 2024: Japan—Trends & Developments*. Chambers Global Practice Guides. London: Chambers and Partners, 2024.

Lumelsky, Avi. “CVE Funding Almost Expired: What You Need to Know.” *Oligo Security Blog*, April 16, 2025.

Maritime Cyber Security. “The Geneva-Based Shipping Company MSC Suffered a Cyberattack.” November 16, 2024. <https://maritimecybersecurity.nl/incident/8dAmdAezDM>

Merriam-Webster. “Vulnerable.” *Merriam-Webster Dictionary*. Accessed February 27, 2025.

Nautilus International. “Cyber Defence: How a New Workbook Aims to Help Seafarers Tackle Tech Attacks.” <https://www.nautilusint.org/en/news-insight/telegraph/cyber-defence-how-a-new-workbook-aims-to-help-seafarers-tackle-tech-attacks/>.



PricewaterhouseCoopers (PwC) Indonesia. "NLE Implementation Hindered by Infrastructure." *Infrastructure News*, July 2024.

Ruiz, Felipe. "Attacks against the Transportation Sector: 10 Recent Critical Security Breaches." *Fluid Attacks Blog*, February 6, 2025.

Sayapin, Sergey. "International Law for a Fragile World: Global Risk and the Limits of Classical International Law." *Opinio Juris*, February 6, 2026.
<https://opiniojuris.org/2026/02/06/international-law-for-a-fragile-world-global-risk-and-the-limits-of-classical-international-law/>.

Vaarandi, Risto, et al. "A Systematic Literature Review of Cyber Security Monitoring in Maritime." *arXiv preprint arXiv:2503.18173v3* (2025).