

## The Legal Frameworks for Cooperative *Internasional Ship and Port Facility Security Code* Implementation to Address Port Security Incidents

Mexi Miano Ubjaan

Email: miano.mexi@gmail.com

Magister Hukum, Universitas Hang Tuah Surabaya,  
Indonesia

---

### Article Info

Received: 2023-02-20

Revised: 2023-06-28

Accepted: 2023-11 -28

### Keywords:

*International Ship and Port Facility Security Code; SOLAS Chapter XI-2; port security; maritime security governance; legal and institutional frameworks*

---

### Abstract

*This conceptual study examines how national legal and institutional frameworks can translate the International Ship and Port Facility Security (ISPS) Code into cooperative, operational practice to prevent, detect, and respond to port security incidents. The paper situates ISPS within contemporary hybrid risk kinetic disruptions to sea lanes, transnational crime, and escalating cyber threats and argues that outcomes depend less on “paper compliance” than on domestic laws and institutions that enable interoperability among public authorities and industry actors. The objective is to develop a practical model aligning legal mandates, institutional roles, and cooperation mechanisms across prevention, preparedness, response, and recovery. Methodologically, the study adopts a qualitative, normative–juridical design with comparative policy and documentary analysis to map (i) the international framework (SOLAS XI-2/ISPS), (ii) Indonesia’s legal-institutional arrangements, and (iii) cooperation mechanisms in practice (information-sharing, inspections/joint patrols, training, intelligence, Declarations of Security, incident command). Empirically grounded discussion highlights budgetary constraints and the value of international cooperation resource sharing, regulatory harmonization, and enhanced coordination for strengthening ISPS implementation. The paper organizes mechanisms against threat categories (violence, legal-violation crime, terrorism) to assess fit-for-purpose alignment and identify interoperability gaps. The contribution is a design blueprint specifying minimum legal features, institutional options, and process enablers (SOPs, joint exercises, audits, feedback loops) to improve cooperative ISPS implementation, with Indonesia as the primary reference case and adaptable guidance for similar jurisdictions.*

---

## **I. INTRODUCTION**

Global maritime trade depends on the continuous, safe functioning of ships and port facilities. Yet ports are open, complex systems where public authorities, private terminal operators, shipping companies, and an array of service providers interact often under time pressure and with tightly coupled digital physical processes. Since 1 July 2004, the International Ship and Port Facility Security (ISPS) Code adopted under SOLAS Chapter XI-2 has provided a common baseline for maritime security through a blend of mandatory requirements (Part A) and implementation guidance (Part B). The Code operationalizes risk management through security assessments and plans for ships and port facilities, designated security officers, graded security levels, and verification by flag and port States (Edgerton, 2013; Jain, 2004). However, translating these global standards into effective practice hinges on national legal and institutional arrangements that enable genuine cooperation among agencies and industry

Contemporary port security challenges are increasingly hybrid combining kinetic, criminal, and cyber vectors and they spill across jurisdictions. Since late 2023, attacks by Yemen's Houthi movement in and around the Red Sea have disrupted a critical artery of global trade, forcing widespread rerouting around the Cape of Good Hope and driving up shipping costs and schedules. The ripple effects have been observed far from the conflict zone e.g., traffic surges at alternative European ports while multinational naval missions have mobilized to protect shipping. These developments underscore how ports must adapt to fast-moving geopolitical risks that directly affect security postures, resource allocation, and incident coordination frameworks at national and port-facility level (Jain, 2004; Kuhn et al., 2023).

Cyber risk has simultaneously become a first-order port security concern. Incidents at major ports including a 2024 attack on the Port of Seattle demonstrate how malicious actors can degrade operations, disrupt logistics data flows, and erode public trust. In response, the International Maritime Organization (IMO) has issued and updated high-level guidance on maritime cyber risk management, complemented by industry guidelines that emphasize governance, risk, and controls integration across ship-shore interfaces. For many States, the immediate challenge is not the absence of guidance, but the need for legal clarity and institutional mechanisms that drive coordinated implementation across port authorities, coast guards, customs, police, terminal operators, and critical-infrastructure agencies (Kuhn et al., 2023; Watts, 2005).

At its core, the ISPS Code frames security as a risk management problem: threats and vulnerabilities must be assessed, plans developed, and measures calibrated to security levels. Yet the Code's effectiveness depends on how States transform this architecture into domestic law and how institutions interact in practice. This raises theoretical questions about multi-level governance (international-national-local), polycentric coordination among agencies, and the balance between hard law (mandatory rules, enforcement

powers) and soft law (guidance, standards, memoranda of understanding). For example, the United States implements ISPS requirements alongside the Maritime Transportation Security Act (MTSA), with the U.S. Coast Guard exercising regulatory and oversight functions and engaging foreign port assessments an illustration of how legal allocations of authority shape inter-agency cooperation and international interface. More broadly, the risk-based logic of ISPS (Part A) and its guidance (Part B) implies that legal frameworks should institutionalize joint risk assessment, information-sharing, and coordinated drills, rather than treating compliance as a siloed checkbox exercise (Fagbore et al., 2024; Nandan Prasad, 2024; Watts, 2005).

A second theoretical issue concerns systems coupling between cyber and physical layers. Port security institutions historically evolved to address physical threats (e.g., unauthorized access, stowaways, sabotage). Today, the same access controls, surveillance systems, and communications that underpin ISPS measures rely on digital infrastructure susceptible to cyber compromise. The IMO's cyber guidance therefore pushes a governance shift: integrating cyber risk into existing safety and security management systems, elevating accountability to senior leadership, and aligning with recognized standards (e.g., ISO/IEC 27001). Legal frameworks that merely require a "plan on paper" are insufficient; they must mandate roles, responsibilities, and minimum capabilities for cross-domain incident response, together with protections for data sharing and joint investigations (Chandersekaran et al., 2008; Flournoy & Schlipper, 2013; Quintana et al., 2012).

Empirical studies have examined ISPS implementation from multiple angles. Case evidence from European ports reports tangible improvements in access control, area surveillance, and workplace security following ISPS adoption, albeit with operational trade-offs. Research in West Africa has associated compliance with enhanced market standing and reduced turnaround times, suggesting downstream performance effects when security regimes are credible and predictable (Marc et al., 2015). Recent work also highlights divergence in awareness and perceived importance of ISPS across stakeholder groups, indicating that "paper compliance" can mask uneven implementation cultures within the same jurisdiction. Collectively, this literature suggests that ISPS can work but its outcomes hinge on local institutional capacity, resources, and cooperative behaviors among actors who share the waterfront.

Beyond effectiveness outcomes, several contributions unpack the risk analysis and governance underpinnings of port security. Studies outline analytical frameworks linking threat identification, vulnerability mapping, and consequence analysis to security planning at facilities, while legal-policy reviews emphasize that ISPS was always intended as a cooperative regime spanning contracting governments and industry, not a purely governmental mandate. Still, compared with technical and operational evaluations, there remains a relative scarcity of research that systematically maps how domestic legal instruments (laws, regulations, directives), institutional setups (competent authorities, inter-agency committees), and formal cooperation tools (MoUs, data-sharing agreements,

joint exercises) interact to produce or impede effective, coordinated responses to security incidents and objectives of the study (Griffiths, 2022)

Against this backdrop, the central problem addressed in this study is how national legal and institutional frameworks can be designed to translate the ISPS Code's risk-based architecture into sustained, cooperative practice among multiple public and private actors at ports. The recent surge of hybrid threats kinetic disruptions to major sea lanes, sophisticated cyber intrusions, and hazardous-materials incidents reveals that "minimum compliance" with plan-and-officer requirements is no longer sufficient. What matters is whether laws and institutions foster interoperability: timely intelligence exchange, joint risk assessments, layered defenses aligned to security levels, harmonized SOPs across agencies, coordinated drills and exercises, and clear command-and-control during incidents. This study, therefore, reframes ISPS implementation from an organizational compliance problem to a cooperative governance challenge situated within each State's legal order.

The purpose of this conceptual study is to examine how national legal and institutional frameworks can operationalize cooperative implementation of the International Ship and Port Facility Security (ISPS) Code to prevent, detect, and respond to port security incidents, and to develop a practical model that aligns legal mandates, institutional roles, and inter-agency/industry cooperation mechanisms.

## **2. RESEARCH METHOD**

This study employs a qualitative, normative juridical design supplemented by comparative policy analysis and documentary content analysis to examine how SOLAS Chapter XI-2 and the ISPS Code are translated into domestic legal instruments and institutional mandates, with structured, focused comparison to illustrative jurisdictions (e.g., the US MTSA/USCG model) and cooperation practices (e.g., Indonesia–Singapore). Normative juridical design is a method that studies law as a set of norms focusing on what the law *is* and *ought to be* by analyzing authoritative legal texts rather than collecting field data (Johnny Ibrahim, 2005; Syahrudin, 2022). The analysis operates at three levels: (1) the international framework (ISPS Parts A–B, security levels, plans, designated officers, verification/control); (2) Indonesia's national legal institutional framework (constitutional aims, Law No. 24/2000 on treaty ratification, sectoral regulations and agency roles across port authority, coast guard, customs, police, terminal operators); and (3) cooperation mechanisms in practice (information exchange, inspections and joint patrols, training and education, intelligence sharing, maritime assistance, Declarations of Security, incident command). Data are desk-based and drawn from international instruments and guidance, domestic laws and regulations, institutional materials (mandates, SOPs, public reports), and scholarly and policy literature. Purposive, criterion-based selection prioritizes texts that establish mandates, responsibilities, and cooperation procedures aligned to four objectives: legal basis, institutional arrangements, cooperation mechanisms, and a model framework. Documents are coded with a standardized extraction template capturing legal

authority, institutional design, cooperation tools, threat alignment (violence; legal violations such as trafficking/smuggling; terrorism), cyber-physical integration, and resourcing/sustainability provisions. The analytical strategy combines doctrinal assessment of conformity and gaps, governance mapping of actors and coordination nodes, a mechanism threat matrix to evaluate fit-for-purpose alignment, structured comparison using common questions (mandates, plan approval/verification, enforcement, intelligence protocols, cyber integration, resource models), and synthesis into a design blueprint specifying minimum legal features, institutional options, and process enablers (SOPs, exercises, audits, feedback loops). Validity and reliability are supported through source triangulation, optional double-coding for codebook stability, and a transparent citation log to preserve the chain of evidence. Ethics considerations include exclusive use of public materials and abstraction of sensitive operational details; no human subjects are involved.

### **3. RESULTS AND DISCUSSION**

#### **3.1. The concept of *Internasional Ship and Port Facility Security Code Cooperation Agreements***

An International Ship and Port Facility Security cooperation agreement between two or more countries is an agreement aimed at enhancing the security of ships and port facilities in each country. This agreement is based on the *International Convention for the Safety of Life at Sea* (SOLAS), which was adopted by the International Maritime Organization (IMO) in 2002. The primary objective of an ISPS cooperation agreement is to prevent and detect acts of terror that could endanger ships and port facilities. The agreement also aims to strengthen cooperation among states in matters related to ship and port facility security. The scope of an ISPS cooperation agreement includes, among other things (Aggarwal et al., 2007):

**a. Exchange of information and data.**

Mutual exchange of information and data related to the security of ships and port facilities. Such information and data may include details on ships, ports, and security threats.

**b. Cooperation in surveillance and inspection.**

States will cooperate in the surveillance and inspection of ships and port facilities. This cooperation may include joint patrol operations, ship inspections, and inspections of port facilities.

**c. Cooperation in training and education.**

States will cooperate in training and education concerning the security of ships and port facilities. This may include organizing training and education programs, exchange experts, and developing training curricula. Examples of ISPS cooperation between Indonesia and Singapore include the exchange of information on ships sailing between the two countries covering a vessel's identity, voyage route, and cargo alongside coordinated ship inspections

involving document verification, physical checks, and cargo examinations. In addition, both states collaborate on training and education for ship and port facility security by organizing joint courses and exercises, facilitating the exchange of experts, and developing shared training curricula.

The following are provisions governing the ratification of international treaties in Indonesia:

- a. Article 10 of Law Number 24 of 2000 on International Treaties
  - (1) International treaties that have been ratified by the President and promulgated by the Minister of Law and Human Rights have binding legal force and constitute part of Indonesian law.
  - (2) International treaties that have been ratified by the President and promulgated by the Minister of Law and Human Rights may not conflict with the 1945 Constitution of the Republic of Indonesia and other laws and regulations.
- b. Article 11 of Law Number 24 of 2000 on International Treaties
  - (1) International treaties that have been ratified by the President and promulgated by the Minister of Law and Human Rights apply throughout the territory of the Unitary State of the Republic of Indonesia.
  - (2) The provision referred to in paragraph (1) does not apply to international treaties that apply only to part of the territory of the Unitary State of the Republic of Indonesia.

### **3.2. Sectors and Mechanisms of Cooperation**

As noted above, security diplomacy must be able to identify and optimally leverage opportunities for cooperation. To identify potential areas of cooperation with other countries, Indonesia must first understand its own national security needs. This can be done by determining which security issues and threats are national priorities and which national capacities need to be strengthened. Doing so will facilitate the conduct of diplomacy at the regional and international levels.

#### **Security Cooperation Sectors.**

In general, national security priority issues can be derived from the forms of Indonesia's maritime security threats, as described in the focus of this study (Dyekman, 2007; Epstein, 2018; Shchokin et al., 2023). Based on these threats, Indonesia can determine forms of cooperation that can be identified and pursued with partner countries. The following is an identification of several potential security cooperation sectors that can be developed:

Tabel 1.

**Security Cooperation Sectors Based on Threat Issues**

| No | Types of Threats  | Examples of Threats                                  | Forms/Opportunities Cooperation sector                                                                                    |
|----|-------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 1  | Violent Threats   | - Piracy<br>- Armed Robbery<br>- Sabotage            | -Law enforcement cooperation<br>-Intelligence cooperation<br>-Emergency assistance                                        |
| 2  | Criminal Offenses | -Human trafficking<br>-Illegal smuggling of persons  | -Law enforcement cooperation<br>-Maritime Governance                                                                      |
| 3  | Terrorism Threats | - Suicide Attack<br>-Use of sea mines<br>-Kidnapping | - Cooperation and exchange of intelligence information<br>-Socialization of security measures to handle acts of terrorism |

The table above illustrates the sectors of security cooperation based on the types of threats faced in the maritime domain. First, in dealing with violent threats such as piracy, armed robbery, and sabotage at sea, the cooperation sector involves law-enforcement efforts. This includes inter-state collaboration to address crimes at sea against ships, coordinating joint patrols, and providing emergency assistance when required. In addition, intelligence cooperation is pivotal for identifying and preventing potential threats to ship and port security.

Threats of legal violations, such as the criminal offenses of human trafficking and the illegal smuggling of persons, call for cooperation focused on law enforcement and maritime governance. States can collaborate in handling criminal acts at sea, strengthening maritime policies, and improving coordination in maritime governance to address these problems. Cooperation in this sector aims to create a secure maritime environment and ensure compliance with international law in marine waters.

Terrorism threats, including suicide attacks, the use of naval mines, and kidnappings, require more intensive cooperation in the exchange of intelligence

information and the implementation of effective security measures. Inter-state collaboration to socialize security measures and to build capacity to counter acts of maritime terrorism against ships and ports is essential. Accordingly, security cooperation sectors based on these threat issues reflect joint efforts to maintain security and stability in national and international port areas.

The conduct of diplomacy cannot proceed in isolation without the support and input of national stakeholders. Therefore, the security cooperation sectors described above are naturally open to further input. Moreover, solid national coordination and communication are needed regarding the identification of appropriate security cooperation sectors and mechanisms that align with national maritime needs and interests. Through such coordination, Indonesia is expected to determine the right, effective, and efficient diplomatic instruments to support the handling of national maritime security challenges.

### **Security Cooperation Mechanisms**

In building cooperation in the priority sectors outlined above, there are several security cooperation mechanisms that can be realized through diplomacy. One avenue for maritime cooperation is financial assistance for the development of port surveillance facilities and technology. However, cooperation mechanisms are not limited to financial and funding assistance; they can also take the form of cooperation related to education and training, military activities, research, and so forth. These forms of cooperation are crucial for enhancing national human-resource capacity to support maritime security and the vision of Indonesia as a Global Maritime Fulcrum (Poros Maritim Dunia). In addition, security cooperation need not occur only at the governmental level; it can also involve the academic community and scientific institutions connected to the maritime sector. In this way, security diplomacy can become more participatory and inclusive. Furthermore, the involvement of the private sector and civil society plays an important role in ensuring diplomacy is carried out effectively and beneficially for national security interests. Below are several security cooperation mechanisms that Indonesia can implement:

#### **1) Port Visits**

Threats to the safety of maritime transport are not limited to natural hazards; they also arise from criminal acts such as terrorism, piracy, human trafficking, and other illegal activities. It is therefore important for international hub ports to raise port-security standards, including by meeting the requirements of the International Ship and Port Facility Security (ISPS) Code. Through reciprocal port visits, the implementation of the ISPS Code can be strengthened because states can discuss port security practices and the protection of transport systems as well as the monitoring of international maritime activities.

#### **2) Personnel Exchanges**

Personnel exchanges can be conducted between law-enforcement officers of one country and another. These activities aim to conduct training, gain operational

experience, and share knowledge and expertise.

3) Maritime Assistance

Implemented by providing support to enhance a country's maritime security. Examples include cooperation to establish a national coast watch center, a coast guard training center, and maritime monitoring and radar facilities. In addition to physical assistance, maritime assistance is also used as an instrument to develop skills such as the ability to detect, understand, respond to, and report maritime activities.

4) High-Level Maritime Strategic Interactions

Conducted through enhanced strategic communication among stakeholders and senior government officials such as sharing each state's maritime perspectives and policies. Beyond physical assistance, these interactions can facilitate operational cooperation through inter-state coordination to strengthen regional maritime security. One example of operational cooperation is joint patrols along shared borders. Such activities are regarded as effective in preventing IUU fishing, illegal trafficking, smuggling of goods, and other maritime crimes. As a form of confidence-building measure, this strategic communication also serves to identify common national interests that can be followed up through concrete maritime security cooperation.

**Bilateral Cooperation**

For bilateral cooperation, as noted, maritime security cooperation involves two states and is built on aligned interests. Bilateral cooperation is viewed as more productive because it avoids the complexity of competing interests and memberships that often characterizes larger groupings. Moreover, the parties involved can more easily set concrete cooperation targets. To facilitate maritime security diplomacy at the bilateral level, Indonesian diplomatic missions can be leveraged to identify the maritime interests of the accrediting state and match them with Indonesia's national maritime cooperation needs. Diplomacy should also ensure that bilateral cooperation contributes to maritime stability and security and to the development of national human capital and maritime technology.

International cooperation is an inter-state relationship whose objectives are anchored in national interests. It consists of a set of rules, principles, norms, and decision-making procedures that govern the functioning of international regimes. States that engage in international cooperation share common objectives or common interests indeed, cooperation without any shared interests would be impossible.

According to K. J. Holsti, cooperation initially arises because various national, regional, and global problems emerge that demand attention from more than one state (K. Holsti, 2016; K. J. Holsti, 2009, 2015). Each state then approaches the problem by bringing proposals or suggestions for solutions, conducting negotiations or bargaining, holding consultations, drawing conclusions from the evidence gathered to justify one of the proposals put forward, and ultimately concluding an agreement that satisfies all parties.

### **3.3. Implementation of the ISPS Code in Indonesia**

The ISPS Code has evolved significantly since it entered into force in 2004. Nevertheless, several challenges remain for its implementation in Indonesia, one of which is budget constraints. Implementing the ISPS Code requires substantial funding, so a long-term government commitment is needed to ensure budgetary continuity (Gunawan et al., 2019; Hendrapati, 2015; Santoso, 2021). One way to address these constraints is through international cooperation. By sharing resources and information among states, the financial burden on each country can be reduced. International cooperation can also enhance the effectiveness and efficiency of ISPS Code implementation by promoting the standardization and harmonization of regulations on ship and port security. Some benefits of international cooperation for ISPS implementation include:

- 1. Greater availability of resources and information.**

International cooperation enables sharing of resources and information such as security equipment and technology, training and certification, as well as intelligence data. This can help Indonesia overcome budgetary and resource limitations in applying the ISPS Code.

- 2. Improved effectiveness and efficiency.**

Cooperation can drive the standardization and harmonization of rules in ship and port security. This helps Indonesia implement the ISPS Code more effectively and efficiently, thereby better protecting the security of ships and ports.

- 3. Enhanced cooperation and coordination among states.**

International cooperation strengthens inter-state collaboration and coordination to improve maritime security, enabling Indonesia to address threats to ships and ports more effectively.

Based on these benefits, collaboration between Indonesia and other countries in implementing the ISPS Code is crucial. International cooperation can help Indonesia address budget constraints, improve the effectiveness and efficiency of implementation, and boost cooperation and coordination among states to enhance ship and port security.

Forms of cooperation that Indonesia may pursue include sharing resources and information through activities such as training and certification, the exchange of intelligence data, and technical cooperation in ship and port facility security participating in international cooperative bodies such as the International Maritime Organization (IMO) and the Asia-Pacific Economic Cooperation (APEC), and concluding bilateral or multilateral agreements with other countries in the field of maritime security.

The choice of cooperation modality should be tailored to each country's needs and circumstances. In principle, the cooperation must deliver tangible benefits to both parties. These international agreements cannot be separated from the state's purposes and interests in managing its relations with other states so as to meet the needs of its people and citizens. The objectives of Article 33 (2) and (3) of the 1945 Constitution of the Republic of Indonesia are to enhance the welfare of all Indonesians and to ensure equitable development across the Republic, particularly throughout Indonesia.

Indonesia needs to cooperate with other countries because of economic interdependence; consequently, multilateral, regional, and bilateral International Ship and Port Facility Security (ISPS) cooperation is required. As we can observe today, Indonesia has established international ISPS cooperation and implements international agreements that play a very important role.

Several aspects of international treaty agreements have served as models for subsequent arrangements and are widely recognized by many countries. In accordance with the principle of *pacta sunt servanda* in international treaty law, every state that concludes a treaty must uphold and comply with its obligations (Schmalenbach, 2017; Situmorang, 2020). This means each treaty must be observed by every state that becomes a party, forming binding norms and fostering cooperation based on the good faith of each party.

For all the reasons above, it is clear that Indonesia must engage in cooperation with foreign states. Such cooperation can help Indonesia enhance potential economic growth and development, improve public services, strengthen national security, and protect the environment. By acting as a responsive participant in international cooperation, Indonesia can help create a safer and more advanced world.

#### **4. Conclusion**

This study reframed implementation of the International Ship and Port Facility Security (ISPS) Code from a narrow exercise in formal compliance to a broader challenge of cooperative governance anchored in domestic law. Ports operate at the junction of public mandates and private operations; therefore, outcomes depend on legal clarity, institutional design, and repeatable mechanisms that enable information-sharing, joint action, and accountable oversight across the ship shore interface. Mapping threats violence at sea, criminal violations such as trafficking and smuggling, and terrorism against concrete cooperation tools demonstrates that effectiveness arises when mandates, processes, and capabilities are intentionally aligned to specific risk profiles rather than treated generically.

The analysis highlights four pillars for a robust framework: (1) a clear legal basis that incorporates SOLAS XI-2/ISPS while empowering inter-agency coordination and industry participation; (2) an institutional architecture with an identified lead authority, defined roles for port authorities, coast guard, customs, police, and operators, and permanent coordination bodies; (3) operational mechanisms intelligence exchange, joint patrols and inspections, training and exercises, Declarations of Security, and incident command that are rehearsed, audited, and continuously improved; and (4) integration of cyber risk into port-security planning, incident response, and assurance regimes. Budget constraints remain real, but international cooperation resource sharing, standards harmonization, and capacity-building can ease fiscal pressure while lifting performance. For Indonesia, priority actions include codifying cooperation duties and data-sharing protections; establishing a single coordinating node with authority over preparedness and response; institutionalizing joint drills and after-action reviews; adopting measurable performance indicators; and leveraging bilateral, regional, and multilateral partnerships (e.g., port visits, personnel exchanges, maritime assistance) to accelerate capability gains. These steps should be supported by sustainable funding and professional development pathways for security officers

across government and industry. Finally, this is a conceptual, normative juridical inquiry; future work should pair the proposed design with empirical validation multi-port case studies, drill evaluations, and cyber-physical exercises to test causal pathways and refine metrics. Even so, the blueprint offered here provides actionable, legally grounded guidance to make ISPS implementation more cooperative, interoperable, and resilient thereby strengthening port security and safeguarding the maritime commerce on which national welfare depends.

## References

- Aggarwal, V., Feldmann, A., & Scheideler, C. (2007). Can ISPs and P2P users cooperate for improved performance? *ACM SIGCOMM Computer Communication Review*, 37(3), 29–40.
- Chandersekaran, C., Simpson, W., & Trice, A. (2008). Cross-domain solutions in an era of information sharing. *The 1st International Multi-Conference on Engineering and Technological Innovation: IMET2008, Orlando, FL, 1*, 313–318.
- Dyckman, G. J. (2007). *Security Cooperation: A Key to the Challenges of the 21st Century*. JSTOR.
- Edgerton, M. (2013). *A Practitioner's guide to effective maritime and port security*. John Wiley & Sons.
- Epstein, S. (2018). *US security assistance and security cooperation programs: overview of funding trends*.
- Fagbore, O. O., Ogeawuchi, J. C., Ilori, O., Isibor, N. J., Odetunde, A., & Adekunle, B. I. (2024). *Building Cross-Functional Collaboration Models Between Compliance, Risk, and Business Units in Finance*.
- Flournoy, R. D., & Schlipper, L. M. (2013). Cross-domain information sharing for next generation interagency experimentation: possibilities and challenges. *The Journal of Defense Modeling and Simulation*, 10(3), 297–312.
- Griffiths, C. T. (2022). Interagency Communication, Collaboration, And Interoperability Within Police Services And Between Police Services And Other Emergency Services. *School of Criminology, Simon Fraser University*.
- Gunawan, E., Zauhar, S., Sarwono, S., & Bambang, S. (2019). The implementation of ship and port facility security policy based on ISPS code at PT Pelindo II (Cirebon branch). *Journal of Management History*, 25(1), 67–96.
- Hendrapati, M. (2015). International Ship and Port Facilities Security Code and Its Implementation in Indonesia. *JE Asia & Int'l L.*, 8, 259.
- Holsti, K. (2016). *Kalevi Holsti: Major Texts on War, the State, Peace, and International Order* (Vol. 42). Springer.
- Holsti, K. J. (2009). From states systems to a society of states: the evolution of international relations. *International Relations*, 1, 75–98.
- Holsti, K. J. (2015). *Why nations realign: Foreign policy restructuring in the postwar world*. Routledge.
- Jain, R. (2004). A model for standardizing risk assessment for port security. *Hoboken, NJ: Stevens Institute of Technology*.
- Johnny Ibrahim. (2005). *Teori dan Metode Penelitian Hukum Normatif*. Bayumedia Publishing.
- Kuhn, K., McIlhatton, D., Malcolm, J. A., & Chapsos, I. (2023). Protective security at sea: A counter terrorism framework for cruise and passenger ships. *WMU Journal of Maritime Affairs*, 22(3), 345–363.
- Marc, A., Verjee, N., & Mogaka, S. (2015). *The challenge of stability and security in West Africa*. World Bank Publications.

- Nandan Prasad, A. (2024). Regulatory Compliance and Risk Management. In *Introduction to Data Governance for Machine Learning Systems: Fundamental Principles, Critical Practices, and Future Trends* (pp. 485–624). Springer.
- Quintana, E., Mackowski, J., & Smith, A. (2012). *Cross-Domain Operations and Interoperability*. Royal United Services Institute.
- Santoso, B. (2021). *The implementation of the International Ship and Port Facility Security (ISPS) Code in Indonesia*.
- Schmalenbach, K. (2017). Article 26: Pacta sunt servanda. *Vienna Convention on the Law of Treaties: A Commentary*, 465–492.
- Shchokin, R., Soloviov, O., & Tantsiura, I. (2023). Strengthening Cooperation between the Civilian and Military Sectors In the Context of State Security: Benefits and Challenges. *Revista de Cercetare Si Interventie Sociala*, 83.
- Situmorang, M. (2020). The Power of Pacta Sunt Servanda Principle in Arbitration Agreement. *Jurnal Penelitian Hukum De Jure*, 21, 447–457.
- Syahrum, M. (2022). *Pengantar Metodologi Penelitian Hukum: Kajian Penelitian Normatif, Empiris, Penulisan Proposal, Laporan Skripsi dan Tesis*. CV. Dotplus Publisher.
- Watts, R. B. (2005). *Maritime critical infrastructure protection: multi-agency command and control in an asymmetric environment*.

