International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Reforming Security Governance for Strategic National Vital Objects: The Case of Kijing International Port, Indonesia

Sutrisno[1], Siti Nurbaiti[2], Sri Bakti Yunari[3]

[1]Doctoral Program in Law, Faculty of Law, Universitas Trisakti, Jakarta, Indonesia
Email: *sutrisnoanantahira41[at]gmail.com*

[2]Promotor, Faculty of Law, Universitas Trisakti, Jakarta, Indonesia

[3]Co-Promotor, Faculty of Law, Universitas Trisakti, Jakarta, Indonesia

Abstract: ***Kijing International Port is strategic infrastructure supporting international trade, industrial development, and logistics connectivity in West Kalimantan, Indonesia. Its security governance involves several institutions operating under separate statutory mandates, resulting in fragmented authority and limited institutional integration. This study examines the existing regulatory framework, its implementation, and the reforms required to establish integrated port security governance. Using normative legal research with statutory, conceptual, and comparative approaches, the study analyses legal materials qualitatively, supported by interviews with relevant institutional actors. The findings indicate that Indonesia possesses extensive sectoral regulations and established security institutions but lacks an integrated legal framework for inter-agency coordination, operational command, information exchange, joint risk assessment, cybersecurity, and collective accountability. Consequently, security governance remains predominantly multi-agency rather than fully integrated. The study proposes a two-tier reform involving statutory harmonisation through the omnibus method and an implementing Presidential Regulation on Integrated Port Security Governance. This framework would strengthen coordination, information sharing, and threat-based operational leadership while preserving the statutory authority of participating institutions.***

Keywords: Port Security Governance; National Vital Objects; Regulatory Harmonisation; Inter-Agency Coordination; Integrated Port Security Governance

1. Introduction

Ports are critical components of national infrastructure because they connect transportation, logistics, international trade, industrial activity, and the movement of people and goods. Their functions now extend beyond conventional loading and unloading. Modern international ports operate as complex economic and digital ecosystems that depend on interconnected infrastructure, information systems, cross-border services, and multiple public institutions.

Kijing International Port in Mempawah Regency, West Kalimantan, reflects this transformation. It was developed as part of Indonesia's strategic port infrastructure and supports industrial development, export-import activity, logistics networks, and major commodities in West Kalimantan. Its geographical position near an international border and international maritime routes also creates exposure to smuggling, customs violations, irregular movement of persons, transnational crime, disruption of port facilities, cyber threats, and risks to strategic infrastructure.

The legal challenge arises from the institutional structure of port security. Security functions are distributed among the Indonesian National Police, Indonesian Navy, Ministry of Transportation, Harbourmaster and Port Authority Office, Sea and Coast Guard Unit, Customs and Excise, Immigration, Quarantine Authority, local government, and PT Pelabuhan Indonesia as the port operator. Each institution derives its authority from different legislation and operates through its own command structure, procedures, information systems, and accountability mechanisms.

Institutional plurality is not inherently problematic. Modern port governance requires specialised institutions. The problem arises when separate statutory powers are not connected by an integrated legal framework. Existing Indonesian rules distribute authority but do not comprehensively regulate coordinating leadership, cross-agency command, interoperable information exchange, joint threat assessment, cybersecurity governance, or collective accountability. This research therefore examines how current security governance is regulated, how those regulations are implemented, and how the regulatory framework should be reformed to establish integrated governance without removing the lawful powers of individual institutions.

2. Literature Survey

2.1 Legal System and Institutional Effectiveness

Lawrence M. Friedman explains a legal system through three interacting elements: legal structure, legal substance, and legal culture[1] . Legal structure concerns the institutions and organisational arrangements through which law operates. Legal substance concerns rules, norms, and institutional mandates. Legal culture concerns values, attitudes, practices, and expectations that influence how legal institutions function.

This framework is relevant to port security because institutional effectiveness cannot be assessed only by identifying whether organisations and regulations exist. A port may have complete institutions and extensive legislation but still experience ineffective governance if authority

remains fragmented, legal rules do not establish inter-agency mechanisms, and institutional cultures continue to favour sectoral interests.

2.2 Authority, Governance, and Institutional Integration

Administrative authority must have a lawful source, defined scope, and identifiable limits. Indonesian administrative law requires governmental authority to remain within legal boundaries[2]. In a port environment, this principle is crucial because different institutions exercise authority within the same operational space. Integration therefore cannot mean transferring all powers to a single institution. It must regulate how distinct statutory powers interact.

Contemporary governance extends beyond hierarchical government. Bevir explains governance through networks, multiple actors, coordination, and changing patterns of public authority[3] . Collaborative governance likewise emphasises structured interaction among public agencies and relevant stakeholders in addressing problems that cannot be effectively managed by one institution[4] . Port governance literature further shows that modern ports depend on coordination among regulatory, operational, logistical, security, and technological functions[5] .

2.3 Comparative Port Security Governance

Comparative governance offers lessons without requiring Indonesia to copy foreign institutional structures. The Netherlands, Japan, and Singapore were selected because each operates a major international port system, uses multi-agency maritime security arrangements, has publicly documented coordination and information-sharing mechanisms, and provides a useful institutional contrast for assessing Indonesia's fragmented port-security governance.

In the Netherlands, the Coastguard coordinates maritime-security information and works with police, customs, port authorities, and other enforcement partners, while the Rotterdam Harbour Master serves as Port Security Officer for the port [6,7]. Japan combines statutory port-facility security with joint inspections involving the police and Japan Coast Guard, providing a useful example of coordinated implementation of international port-security standards [8]. Singapore links multi-agency maritime coordination, information fusion, and operational response through institutions such as the Singapore Maritime Crisis Centre and Information Fusion Centre [9,10].

Across these jurisdictions, four recurring features are relevant to the Kijing case: identifiable coordination arrangements, structured information exchange, command-and-control capacity, and risk-based security management.

3. Problem Definition

The central legal problem is not the absence of institutions or legal authority. Indonesia already has multiple institutions with statutory mandates relevant to port security. The problem is the absence of legal mechanisms that connect these mandates into one coherent governance system.

Three related problems are examined. First, existing regulations remain sectoral and do not sufficiently define inter-agency relationships, coordinating leadership, integrated command, information interoperability, joint risk assessment, or integrated audit. Second, implementation depends heavily on administrative coordination and situational cooperation rather than permanent institutional mechanisms. Third, the legal framework does not yet provide an adaptive command arrangement for changes in the type and level of threat, particularly the transition from normal civilian security conditions to cross-sector incidents or defence-related threats.

4. Methodology / Approach

This research uses a normative legal research design with a descriptive-analytical character. Law is examined as a system of norms, principles, doctrines, institutional powers, and regulatory relationships governing the security of strategic national infrastructure.

Three approaches are applied. The statutory approach examines rules governing national vital objects, policing, defence, shipping, customs, immigration, quarantine, government administration, cybersecurity, and international port security [11–19]. The conceptual approach uses legal system theory, authority theory, institutional theory, governance, and collaborative governance. The comparative approach examines the Netherlands, Japan, and Singapore using four common assessment dimensions: institutional coordination, information exchange, command-and-control arrangements, and risk management[20] .

The comparative cases were purposively selected because they combine high-volume international port activity with documented multi-agency security governance and formal mechanisms for coordination or information sharing. The purpose of the comparison is analytical rather than transplantational: it identifies governance mechanisms that may be adapted to the Indonesian legal context.

The principal research materials consist of primary, secondary, and tertiary legal materials. Primary materials include the Indonesian Constitution, statutes, presidential instruments, police and maritime regulations, and relevant international instruments, including SOLAS Chapter XI-2 and the International Ship and Port Facility Security Code. Secondary materials include books, peer-reviewed articles, official institutional reports, and port-governance studies.

Supporting interviews were purposively directed to institutional actors involved in Kijing Port security and governance. The institutional categories covered the Indonesian National Police, Indonesian Navy, Harbourmaster and Port Authority Office, Sea and Coast Guard Unit, Customs and Excise, Immigration, Quarantine Authority, and PT Pelabuhan Indonesia. Interview material was used to clarify how written legal mandates operate in practice, identify coordination and information-sharing problems, and test the consistency between regulatory design and institutional implementation. Because the interviews serve as supporting material, they do not alter the normative character of the research.

All materials are analysed qualitatively through legal interpretation, systematisation, comparison, and examination of horizontal and vertical regulatory relationships. Conclusions are drawn deductively from general legal principles and statutory arrangements to the specific governance problems at Kijing International Port.

5. Results & Discussion

5.1 Existing Regulatory Framework: Institutional Completeness and Fragmented Authority

Kijing International Port has a relatively complete institutional security structure. The Police exercise public security and law-enforcement functions. The Navy performs defence-related functions under the applicable defence framework. Maritime authorities perform shipping safety and security functions. Customs supervises cross-border goods, Immigration controls the movement of persons, and Quarantine performs biosecurity functions. National Vital Object security is also governed by Presidential Decree No. 63 of 2004.

Institutional completeness has not produced institutional integration. Each organisation remains embedded in a separate statutory and administrative framework. This finding is consistent with institutional theory, which distinguishes formal institutional presence from the deeper regulative, normative, and cultural-cognitive conditions needed for stable inter-organisational behaviour. From Friedman's perspective, the weakness lies not in the absence of legal structure but in fragmented authority within an otherwise complete structure[1] .

The substantive framework follows the same pattern. Indonesia has rules covering national vital objects, policing, defence, shipping, customs, immigration, quarantine, administrative authority, and the ISPS Code. The core weakness is horizontal fragmentation: the rules allocate sectoral powers but do not sufficiently govern their interaction when threats cross institutional boundaries. The main gaps concern a coordinating lead agency, integrated command, permanent joint operations, interoperable information systems, cybersecurity governance, joint risk assessment, and integrated governance audits.

5.2 Implementation: Multi-Agency Governance Without Full Integration

Implementation shows that cooperation already exists. Institutions conduct coordination meetings, communicate operationally, implement ISPS Code requirements, conduct security-management audits, and undertake joint patrols or joint operations when necessary[18] . These practices demonstrate active cooperation, but they remain predominantly administrative and situational.

Each institution continues to operate its own command system and information environment. No permanent integrated command centre combines cross-institutional security functions, while information on vessels, customs, immigration, physical security, maritime surveillance, and terminal operations remains distributed across separate systems. Digitalisation has occurred within individual institutions, but interoperability remains limited. The current arrangement is therefore better characterised as multi-agency security governance than as fully integrated port security governance.

5.3 Comparative Findings

The Dutch case illustrates coordination through the Netherlands Coastguard and port-level security authority in Rotterdam. Security information is analysed before port entry, enforcement partners are connected through defined arrangements, and the Harbour Master acts as Port Security Officer for Rotterdam[6,7] .

Japan demonstrates coordinated implementation of port-facility security under the Act on Assurance of Security of International Ships and Port Facilities. MLIT documents approval of port-security plans and joint inspections with the police, Japan Coast Guard, and other agencies[8] .

Singapore demonstrates a more explicit linkage between maritime situational awareness and operational response. The Singapore Maritime Crisis Centre coordinates national agencies, while the Information Fusion Centre supports actionable information sharing across maritime-security partners[8] .

The comparison yields four lessons for Indonesia. First, institutional plurality requires an identifiable coordination mechanism. Second, information exchange should be structured and timely rather than dependent on ad hoc requests. Third, a command centre should function as a coordination and decision-support mechanism, not merely as a surveillance room. Fourth, operational priorities should be informed by joint risk assessment rather than isolated institutional assessments.

5.4 Two-Tier Regulatory Reform

Regulatory reform should operate at two levels. The first is statutory harmonisation. The current framework is spread across laws governing policing, defence, shipping, customs, immigration, quarantine, government administration, and electronic security. Harmonisation should introduce connecting norms defining inter-agency relationships, information-sharing obligations, threat-escalation mechanisms, joint risk management, and institutional accountability. Where related amendments are required across statutes at the same legislative level, Indonesia's omnibus method can support coordinated legislative reform[19].

The second level is an implementing Presidential Regulation on Integrated Port Security Governance. This instrument should regulate a coordinative lead agency, an Integrated Port Security Command Center, an integrated digital information-sharing platform, joint intelligence, a permanent joint operation centre mechanism, joint risk assessment, integrated physical and cybersecurity governance, cross-agency standard operating procedures, collaborative decision-making, integrated governance audits, and escalation of operational leadership according to the type and level of threat.

5.5 Integrated Port Security Governance as the Outcome of Reform

Integrated Port Security Governance (IPSG) is the principal outcome proposed by this study. It is not a new institution designed to absorb existing legal authority. Its core principle is integration of authority, not centralisation of authority.

IPSG links existing powers through four core mechanisms: a coordinative lead agency, an Integrated Port Security Command Center, an integrated digital platform, and a threat-based operational leadership mechanism. Under normal civilian conditions, institutions exercise their ordinary statutory powers. When an incident becomes a cross-sector security threat, operational leadership adjusts according to the institution legally most relevant to the threat. If the situation escalates into a defence-related threat, leadership and command adjust according to defence law and the applicable legal mechanism.

The framework therefore combines integrated leadership, authority, command, information, intelligence, joint operations, risk assessment, physical and cyber security, audit, collaborative decision-making, and adaptive governance. Its contribution is to provide a legal and institutional bridge between sectoral statutory authority and integrated operational governance.

6. Conclusion

The study concludes that security governance at Kijing International Port is supported by established institutions and extensive sectoral regulations, but lacks an integrated legal and operational framework. Existing statutory arrangements distribute responsibilities among security, defence, maritime, customs, immigration, quarantine, and port management institutions without sufficiently regulating their coordination, information exchange, joint risk assessment, and collective accountability.

Consequently, implementation remains predominantly multi-agency, with coordination dependent on separate institutional procedures and situational cooperation. To address these limitations, the study proposes a two-tier regulatory reform comprising statutory harmonisation through the omnibus method and an implementing Presidential Regulation on Integrated Port Security Governance.

The proposed framework would establish coordinated leadership, integrated information systems, joint operational mechanisms, cybersecurity governance, and threat-based command arrangements while preserving the lawful authority of participating agencies. This approach provides a regulatory foundation for more coherent and adaptive security governance at Kijing International Port and potentially other strategic Indonesian ports.

7. Future Scope

Future research should test the applicability of IPSG at other Indonesian strategic ports with different cargo profiles, international connectivity, infrastructure capacity, and threat environments. Comparative implementation can identify which elements should be nationally standardised and which should remain adaptable to local conditions.

Further research should also develop legal standards for inter-agency data interoperability, cybersecurity responsibility, information classification, incident response, integrated security audits, and measurable threat-escalation indicators. The present study is limited to normative legal analysis centred on Kijing International Port, with interviews used as supporting material. Pilot implementation, simulations, and multi-port empirical evaluation would provide additional evidence regarding institutional effectiveness and regulatory impact.

References

[1] Friedman LM. The Legal System: A Social Science Perspective. New York: Russell Sage Foundation; 1975.
[2] Republic of Indonesia. Law No. 30 of 2014 on Government Administration. n.d.
[3] Bevir M. Governance: A Very Short Introduction. Oxford: Oxford University Press; 2012.
[4] Emerson K, Nabatchi T. Collaborative Governance Regimes. Washington DC: Georgetown University Press; 2015.
[5] Brooks MR., Cullinane Kevin. Devolution, Port Governance and Port Performance. vol. 17. 1st ed. Oxford, Amsterdam, San Diego: 2007.
[6] Coastguard Governance - Netherlands Coastguard n.d. https://kustwacht.nl/en/governance/? (accessed July 28, 2026).
[7] Drones | Port of Rotterdam n.d. https://www.portofrotterdam.com/en/port-future/innovation/drones? (accessed July 28, 2026).
[8] Ministry of Land IT and T of Japan. Ministry of Land, Infrastructure, Transport and Tourism of Japan. White Paper on Land, Infrastructure, Transport and Tourism in Japan 2019: Section 5 Crisis Management and Security Measures [Internet]. Tokyo: MLIT 2019.
[9] Fact Sheet on Information Fusion Centre (IFC) and Launch of IFC Real-Time Information-Sharing System (IRIS) | Ministry of Defence n.d. https://www.mindef.gov.sg/news-and-events/latest-releases/14may19_fs/ (accessed November 10, 2026).
[10] Fact Sheet: Safeguarding Singapore's Maritime Trade and Industry | Ministry of Defence n.d. https://www.mindef.gov.sg/news-and-events/latest-releases/19apr18_fs/ (accessed November 10, 2026).
[11] Republic of Indonesia. Law No. 21 of 2019 on Animal, Fish and Plant Quarantine. n.d.
[12] Republic of Indonesia. Law No. 6 of 2011 on Immigration, as amended. n.d.
[13] Republic of Indonesia. Law No. 10 of 1995 on Customs, as amended by Law No. 17 of 2006. n.d.
[14] Republic of Indonesia. Presidential Decree No. 63 of 2004 on the Security of National Vital Objects. n.d.
[15] Republic of Indonesia. Law No. 17 of 2008 on Shipping, as amended. n.d.
[16] Republic of Indonesia. Law No. 34 of 2004 on the Indonesian National Armed Forces, as amended by Law No. 3 of 2025. n.d.
[17] Republic of Indonesia. Law No. 2 of 2002 on the Indonesian National Police. n.d.

[18] International Maritime Organization. SOLAS XI-2 and the ISPS Code n.d. https://www.imo.org/en/ourwork/security/pages/solas-xi-2%20isps%20code.aspx? (accessed May 13, 2026).
[19] Republic of Indonesia. Law No. 13 of 2022 on the Second Amendment to Law No. 12 of 2011 on the Formation of Laws and Regulations. n.d.
[20] Scott WR. Institutions and Organizations: Ideas, Interests, and Identities. 4th ed. Thousand Oaks: SAGE Publications; 2014