RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore
Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg No. 005 – 10 January 2023

No. 005/2023 dated 10 January 2023

The Maritime Security Roles of Port Authorities in Southeast Asia

Martin Marini

SYNOPSIS

Ports are essential maritime security nodes that must prevent the movement of threats between sea and land. Key among these threats are illicit cargo, criminals and disease. ***MARTIN MARINI*** *notes that as demand for the quick and smooth flow of goods increases in tandem with the growing volume of seaborne trade, port authorities are finding their maritime security duties increasingly challenging. Inter-agency cooperation and modernised electronic systems are helping port authorities rise to the challenge, but the latter also expose them to emerging cyber security threats.*

COMMENTARY

Ports and terminals, particularly those that handle international shipping, are fundamental to maritime security. Port authorities and port operating companies seek to ensure shoreside security of the cargoes, crews and passengers passing through their gates, wharves and anchorages and prevent the entry ashore of shipboard criminals or undesirable elements, illicit goods, and vermin and disease. Preventing ports from becoming transit points for viruses became especially pertinent during the COVID-19 pandemic. Working alongside their national customs, immigration and quarantine (CIQ) agencies, port authorities and port operating companies tend to view port security largely from a shore-based perspective.

Port Authorities' Perception of the Most Significant Maritime Security Threats

Port authorities tend to be most concerned with criminals who target ships, ports and terminals, cargoes, crews, and passengers, as well as financial, personal and corporate data and systems, for their illicit ends. Such illicit ends include smuggling

operations that use these facilities and theft of valuable cargo, equipment and material. Terrorism too is a persistent threat that requires vigilance. Climate change and natural disasters are increasing threats.

The most rapidly emerging threats today involve cyber hackers, with ports and terminals being increasingly reliant on real-time digital documents and data exchanges between themselves and their stakeholders. Customs and immigration authorities, vessel traffic control and pilotage service providers, arriving and departing vessels, port agents husbanding these ships or paying port dues for them, and service providers supplying fuel, water and provisions are just some of the essential stakeholders.

New and added challenges to data and information security for ports could come from amateur hackers or criminal syndicates. They may steal data, compromise data in the process of stealing or diverting containers or cargoes from their intended consignees or shippers, or manipulate data to mask “Trojan containers” or to smuggle illicit cargoes.

The raison d'être of port authorities, that is facilitating the quick and smooth movement of goods does not have to be in contradistinction with the imperatives of maritime security. *Image from Wikimedia.*

Governance of Port Authorities’ Maritime Security Activities

Ports are guided by several important conventions under the International Maritime Organisation (IMO). The 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) is relevant to ports because it prohibits and punishes behaviour threatening the safety of maritime navigation. The International Ship and Port Facility Security (ISPS) Code too imposes specific

requirements on ports. Part A of the Code sets out substantive standards that ports and terminals of ratifying states must meet. Part B provides a series of guidelines on how to meet these standards.

The IMO published the *2012 Guide to Maritime Security and the ISPS Code* to assist state parties to the International Convention for the Safety of Life at Sea (commonly known as SOLAS), port facility personnel, and the wider shipping industry. The guide is comprised of the ISPS Code's non-mandatory Part B, as well as a variety of maritime security–related IMO resolutions, circulars and circulars letters. A comprehensive document, the guide provides recommendations to assist port facility personnel and shipping company employees with security duties in ports and port facilities and on board ships. The ISPS is complemented by the 2003 Joint International Labour Organisation (ILO)/IMO Code of Practice on Security in Ports.

With the rise of cyber risks to port security, a growing number of conventions and circulars have been issued to address such risks. These include the IMO's MSC-FAL.1/Circ.3 circular on *Guidelines on Maritime Cyber Risk Management, the International Organisation for Standardization and International Electrotechnical Commission* ISO/IEC 27001 standard on information technology, and the United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity. They provide recommendations and guidance on maritime cyber risk management and security techniques.

Port Authorities' Contribution to Maritime Security

Ports are gateways that, when properly manged, prevent the flow of illicit actors and goods into a country. They contribute to maritime security by controlling the access points between land and sea and between different countries and actors. Ports put in place different security mechanisms to ensure that illicit flows are limited while at the same time ensuring that licit trade goes on relatively undisrupted.

Port Authorities' Operations in the Maritime Security Environment

Ports historically met various physical challenges by relying on auxiliary police forces and organic fire and rescue personnel and assets, perhaps due to the resource or priority constraints of national authorities. Facilitated by almost universal adoption of the ISPS Code, internationally mandated carriage of transponders by ships, and vessel pre-arrival notification procedures at ports and terminals as a condition of a ship's entry, ports have become essential nodes in global maritime security.

Verifiable and trackable documentation plays an essential part in port authorities and operators' work to ensure security. These documents include vessel pre-arrival or port clearance notifications, dangerous goods declarations, CIQ and crew health declarations, submissions of a ship's trading and insurance certificates, notices to mariners, navigational telegraphy (navtex), and safety broadcasts from ports' vessel traffic information service (VTIS).

Such documentation is increasingly rendered in electronic format. For example, the port of Singapore is almost entirely paperless. The official web portal of PSA Singapore, the operator of Singapore's main container and cargo terminals, refers to

this transition away from paper as "Leverage on technology'". PSA developed the Access Control and Electronic Security (ACES) system to support the security service provider and all staff to raise their security preparedness.

Ports also create a security culture through the use of training, sensitising, drills, and exercises. There is a growing tendency and need to train port workers on the importance of good information technology discipline, as well as the need to report suspicious behaviour.

A final tool that ports use is cooperation and coordination with other stakeholders, who include both security agencies and industry partners. An indicative example is PSA Singapore. They work with domestic security stakeholders such as the Maritime and Port Authority of Singapore (MPA), the Immigration and Checkpoints Authority (ICA) and the Singapore Police Force (SPF) on regulatory requirements, baseline security measures and best practices. These maritime security agencies hold regular joint exercises to test and strengthen their inter-agency procedures and coordination and familiarise their personnel with each other. They also coordinate with global industry stakeholders.

An indicative programme is the Singapore Customs' Secure Trade Partnership Programme, which is consistent with the World Customs Organisation's SAFE Framework of Standards. This supports Singapore Customs' initiatives such as the Cargo Targeting System (CTS), Container Security Initiative (CSI) for US-bound goods and Radiation Detection Initiative (RDI) for export containers.

Port Authorities and Maritime Awareness

Port authorities' greatest contribution to maritime domain awareness involves shipping and lading documentation. Arrival and departure schedules, manifests, insurance documentation, crew lists and other documents provide important data. However, sharing is not always seamless as much of this information is business-sensitive and not all ports have mechanisms for the swift and secure sharing of data.

Within Southeast Asia, the most sophisticated domestic information sharing model is implemented by Singapore's port authority. Within Singapore, the maritime security stakeholders, including civilian, military, commercial and government bodies, have grown into a coherent community sharing similar goals and closely collaborating by both formal and informal means.

For example, as the national port regulator, and on behalf of the state as a contracting government, MPA is required under the ISPS Code to set security levels. MPA ensures that current information on the security threat level is made known to ships operating in and those intending to enter Singapore waters and their respective flag states. MPA does this in close consultation with other national maritime security stakeholders such as the navy, the police and security agencies, and the port terminal operators.

Evolution of Port Authorities' Maritime Security Roles

Global concerns following the 11 Sept 2001 airline hijacking resonated in the thinking of port authorities. The mega-attack scenarios most often envisioned were the smuggling of weapons of mass destruction and the use of hijacked ships and vulnerable port-adjacent facilities such as refineries and gas storage facilities. Operators were also concerned about the prospect of their ports providing entry points for international terrorists. But port authorities' concerns shifted from risk to compliance as the regulations and requirements of the ISPS Code required swift introduction. For some ports, compliance became a costly burden, stretching resources

Despite the ISPS Code, maritime terrorist and security incidents, including the 2008 Mumbai terrorist attacks, demonstrated that ports remained vulnerable. These events clearly demonstrated that port security ashore and maritime security at sea were essentially conjoined twins; any harm to one also hurts the other.

Ports have been increasingly recognised as essential gateways between the land and sea domain domains; consequently, stronger emphasis is placed on security mechanisms (both physical and digital). This means that over the past two decades, port authorities have been increasingly involved in security provision and have become important maritime security partners. They have simultaneously become more willing partners as security issues can have economic consequences for ports.

Additional Context

Ports have complex governance structures. Some ports in the region, such as Indonesia's Tanjung Priok, are owned by state-owned companies or operated by the state themselves, such as Bangkok Port. Others are operated by private companies. Singapore's PSA, for example, is a landlord port where the land is leased from the state.

There is even a strong variation of models within countries — in Johor, Malaysia, Tanjung Pelepas is privately run while Johor port is state-owned. This lack of uniformity results in strong variation in how ports are governed and how well port authorities work with public agencies. This is often a challenging situation, but the success of communication between these different stakeholders is important for port authorities to contribute to maritime security.

A second contextual consideration that arises from private ownership of ports concerns the balance between security provision and economic fluidity. Private port authorities may be primarily concerned with avoiding disruption and facilitating the fast flow of goods, which maritime security provisions may disrupt or slow down.

Martin Marini *was general counsel of the Maritime and Port Authority (MPA) of Singapore from 2005 until he retired on 1 Jan 2020. This IDSS Paper is #10 of 12 from a workshop the RSIS Maritime Security Programme conducted regarding the evolving roles of Southeast Asia's maritime security stakeholders.*

The final report of the workshop is also available online.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg