RSIS COMMENTARY

27 February 2026

Protecting Critical Maritime Infrastructure: A Multi-Domain Approach to Maritime Security Governance

Su Wai Mon

RSiS
S. RAJARATNAM
SCHOOL OF
INTERNATIONAL
STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 033 – 27 February 2026

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Protecting Critical Maritime Infrastructure: A Multi-Domain Approach to Maritime Security Governance

By Su Wai Mon

SYNOPSIS

This commentary examines how emerging threats across physical, cyber, undersea, and space domains are creating unprecedented risks to critical maritime infrastructure. It argues that proactive and coordinated action by industry, regulators, and governments, supported by coherent legal and regulatory frameworks, is essential to strengthening resilience. While the analysis global relevance, the piece highlights Southeast Asia and the Indo-Pacific as a strategic case study, demonstrating the urgent need for integrated, multi-domain, and regional cooperation to tackle evolving maritime security challenges.

COMMENTARY

Good maritime security governance requires an integrated multi-domain approach, given that emerging threats increasingly target critical infrastructure across interconnected terrestrial, digital, maritime and even space domains.

Historically, maritime security threats, whether traditional or non-traditional, were largely confined to the physical maritime domain. Today, however, the maritime threat landscape is rapidly evolving alongside advances in technology, digitalisation, and the automation of maritime infrastructure.

Ships, ports, and offshore infrastructure, such as oil and gas installations and offshore wind farms, form part of increasingly interconnected systems and are all regarded as critical maritime infrastructure. In addition, the communication systems that provide connectivity between them have become essential and therefore warrant stronger protection as critical infrastructure.

For example, space infrastructure, particularly satellites, plays a critical role in maritime operations such as navigation, communication, and surveillance, and its importance will only grow as the shipping industry becomes more reliant on higher-bandwidth connectivity to support advanced technologies, including autonomous ships, artificial intelligence, the Internet of Things, blockchains, and big-data analytics.

In addition, protecting critical underwater infrastructure (CUI), subsea cables, and pipelines is increasingly crucial given their dual physical and digital vulnerabilities and their central role in global connectivity and energy security. As a result, maritime security challenges have increasingly extended beyond the physical maritime domain into the cyber and digital realms.

Cybersecurity and Physical Security Risks in the Maritime Sector

Several reported incidents underscore the growing exposure of critical maritime infrastructure, including ships, ports, satellite systems, as well as subsea cables and pipelines, to both physical and cyber threats, with cyberattacks on digital systems capable of causing substantial effects in the physical domain.

Some of the reported incidents, including ransomware attacks, are the Maersk Notpetya attack (2017), which infected 45,000 PCs and 4,000 servers, leading to the shutdown of 76 global port terminals. Japan’s Nagoya Port was forced to shut down its operations due to a ransomware attack (2023). The DP World Australia cyberattack (2023) led to the closure of port operations in Sydney, Melbourne, Brisbane, and Fremantle.

Additionally, the offshore wind sector has already been exposed to cyber risks, with major companies, such as Enercon, Vestas, Nordex, and Deutsche Windtechnik reporting malware and ransomware attacks. Remote cyberattacks on offshore platforms, including oil rigs and other energy platforms carry the risk of serious human and environmental harm through ruptures, explosions, fires, and spills.

The shipping industry is highly dependent on satellite communication systems, which are increasingly vulnerable to cyberattacks. Disruptions to GNSS/GPS connectivity, particularly spoofing and jamming, have become a growing concern as they can deceive vessels into thinking they are on a safe course while steering them toward hazardous or restricted waters.

In July 2019, the UK-flagged oil tanker, Stena Impero, was seized by Iran while transiting the Strait of Hormuz, with investigations suggesting that its GPS was spoofed, causing it to deviate into Iranian territorial waters.

In another reported incident, vessels operating near Chinese ports experienced widespread GPS anomalies caused by spoofing attacks, affecting hundreds of vessels and disrupting port operations. CYDOME reported that the Lab Dookhtegan attack on Iranian oil tankers successfully disrupted all communications for 116 vessels operated by two Iranian companies, by exploiting vulnerabilities in the maritime satellite communication systems these ships rely on.

Security of Critical Undersea Infrastructure

Critical undersea infrastructure, such as submarine cables and pipelines, faces growing exposure to both physical sabotage and cyber threats. Hybrid operations targeting maritime infrastructure are increasingly blurring the line between peacetime and armed conflict, leaving undersea cables and pipelines vulnerable to a combination of physical interference and cyber activities.

Recent incidents and reports of damage to communication and energy cables worldwide, especially in the Baltic Sea, Red Sea, Taiwan, and Vietnam, underscore these concerns. Submarine cable infrastructure faces serious cybersecurity threats, mainly from the use of remote network management systems (RNMS), which allow operators to monitor and control cable functions remotely, including data flows and power management.

Although RNMS enhance efficiency and reduce costs, their internet connectivity increases exposure to cyber threats, potentially undermining the security and resilience of cable systems, especially through third-party access. This danger was illustrated in April 2022, when US authorities disrupted a cyberattack on a Hawaii undersea cable system that stemmed from compromised third-party credentials.

Existing Legal and Regulatory Challenges

Current regulatory approaches addressing cybersecurity risks to critical maritime infrastructure remain fragmented, with different standards applying to ships, ports, and offshore installations. Furthermore, the integration of terrestrial, maritime, undersea, and space-based infrastructure presents additional regulatory and operational complexities.

Different legal frameworks apply depending on whether a situation is considered peacetime or armed conflict, yet the exposure and vulnerability of critical maritime infrastructure remain largely the same. Many of today's maritime security incidents fall into a grey zone, where activities are intentionally covert or ambiguous, making it difficult to assign responsibility due to challenges in attribution or determine whether legal thresholds for armed conflict have been crossed.

This uncertainty complicates law enforcement and policy responses and highlights the growing challenge posed by increasingly sophisticated and hybrid maritime threats. Recognising and addressing these grey-zone risks is therefore essential for strengthening maritime security and resilience in the current strategic environment.

The United Nations Convention on the Law of the Sea (UNCLOS, 1982) continues to serve as the primary legal framework during peacetime. However, it was drafted in an era that did not anticipate today's technological realities and therefore provides limited guidance on emerging challenges such as the deployment of Maritime Autonomous Surface Ships (MASS), the cybersecurity of critical maritime infrastructure, and the proliferation of unmanned underwater vehicles (UUVs).

Southeast Asia and the Indo-Pacific as a Case Study

Southeast Asia and the broader Indo-Pacific region are increasingly exposed to a wide range of emerging security threats that span multiple domains, including the digital, maritime, and space sectors.

The Straits of Malacca constitutes one of the world's most critical maritime chokepoints, with thousands of vessels transiting annually, carrying strategically important cargos such as oil, liquefied natural gas, and chemical products. At the same time, the region is marked by increased geopolitical tensions, particularly in the South China Sea, which further amplifies vulnerabilities in the maritime domain.

These dynamics have intensified concerns over hybrid threats targeting critical maritime and undersea infrastructure, including ports, shipping, and submarine cables. In this context, regional states face an urgent need to adopt proactive, comprehensive approaches that combine legal, technological, operational, and cooperative measures to address the evolving maritime security challenges in the contemporary security environment.

The Way forward

Waiting for a crisis to take place before responding is no longer a viable option for the maritime sector. Given the increasing sophistication of threats and the evolving nature of maritime operations, existing legal and regulatory frameworks are struggling to keep pace, which shows the need for proactive, coordinated, and cooperative measures at national, regional, and international levels to enhance the resilience and security of critical maritime infrastructure.

Most Southeast Asian countries have yet to develop comprehensive national maritime security policies or strategies. Setting clear priorities is crucial for strengthening the resilience of critical national infrastructure. We need to establish effective coordination and cooperation among relevant national agencies at the domestic level before meaningful regional or international collaboration can take place. Regulators and governments should proactively define critical maritime infrastructure (CMI) across multiple domains and prioritise its protection through the adoption of integrated maritime security strategies.

An integrated multi-domain approach, anchored in clear legal frameworks, strong inter-agency cooperation, and mutual trust between public and private stakeholders, is essential to reinforce regional and international collaboration, protect critical infrastructure, and build resilience against evolving maritime security threats.

Dr Su Wai Mon is a Research Fellow (Ocean Law and Policy) at the Centre for International Law, National University of Singapore, and a former senior lecturer at the Faculty of Law, University of Malaya. Her work focuses on legal and governance implications of emerging technologies in maritime security, maritime cybersecurity, critical maritime and undersea infrastructure governance.

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.