IDSS PAPER

11 March 2026

Protecting Critical Undersea Infrastructure

Accelerating the Momentum in ASEAN

Jane Chan and Nicholas Lim

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

RSiS 30

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.039– 11 March 2026

The authors' views are their own and do not represent the official position of the Institute of Defence and Strategic Studies of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the authors and RSIS. Please email to Editor IDSS Paper at RSISPublications@ntu.edu.sg.

Protecting Critical Undersea Infrastructure: Accelerating the Momentum in ASEAN

Jane Chan and Nicholas Lim

KEY TAKEAWAYS

- *Most incidents of damage to critical undersea communications and energy infrastructure were accidental, but such infrastructure is also vulnerable to sabotage.*
- *A key lesson learnt from the Baltic experience is that Southeast Asian states must cooperate to protect undersea infrastructure.*
- *ASEAN can take a more proactive role in bringing together all parties that have a stake in the protection of such infrastructure.*

COMMENTARY

The importance of submarine communication cables, energy cables and oil and gas pipelines is well known. These are now commonly referred to as critical undersea infrastructure (CUI) and are essentially lifelines to critical services on land such as power, communication and financial services. While most incidents of damage to CUI have been accidental, there have been reports of cases near and far that seem to be acts of sabotage. The *Newnew Polar Bear* incident in the Baltic is a good example. While there are competing accounts of what transpired in the *Newnew* case, the incident exposed a real security vulnerability for all states relying on the undisrupted operation of such infrastructures.

The vulnerability of CUI is often spoken of as an emerging threat, but cutting an adversary state's cables is anything but new. Such tactics have been used as early as during World War I, when the British targeted German undersea telegraph cables. The issues and lessons learnt then – communications infrastructure is a strategic

vulnerability; there is a need for resilience, and repairs involve complexities – are equally applicable today. While legal scholars debate over issues of legitimacy, neutrality and proportionality, how states are choosing to respond to such attacks matters too.

Protection of CUI is increasingly complicated by contemporary maritime practices, such as the use of "dark ships" – ships engaged in illegal activities and flagged in countries with weak governance standards – as well as ships that "spoof" flag registry or identity, both of which compound the already vexing challenges of surveillance and attribution. Moreover, gaps in international law, including the United Nations Convention on the Law of the Sea (UNCLOS), make it difficult to hold perpetrators to account.

The Nordic and Baltic states, having weathered several high-profile incidents, offer a blueprint for regional resilience, especially on what a state and the region can do to protect CUI. These include improved monitoring and surveillance capabilities, protection and repair capabilities, stronger interagency cooperation and coordination, and robust regional mechanisms and partnerships. Many of these ideas are aimed at filling the gaps within the international legal regime that have left coastal states struggling with the lack of enforcement jurisdiction to protect CUI beyond sovereign waters.

Efforts within ASEAN

In Southeast Asia, the issue of CUI protection was discussed as early as 2019, when ASEAN released the ASEAN Guideline for Strengthening Resilience and Repair of Submarine Cables. Five years later, ASEAN's foreign ministers released a Joint Communiqué at the 57th ASEAN Foreign Ministers' Meeting in Vientiane on 25 July 2024, which mentioned the importance of a secure and resilient submarine cable network for regional and global connectivity. This emphasis on the resilience of submarine infrastructure was reinforced in the ASEAN Connectivity Strategic Plan, which was adopted at the 46th ASEAN Summit in Kuala Lumpur under the ASEAN Community Vision 2045. More concrete measures were raised for discussion in the Concept Paper on Critical Underwater Infrastructure (CUI) Security, adopted at the 19th ASEAN Defence Ministers' Meeting (ADMM) on 31 October 2025.

The thrust of the ADMM Concept Paper was that CUI security is a relevant and emerging domain for ASEAN defence establishments and that ASEAN member states need to do more to protect and secure it. While the concept paper also proposed that the economic and telecommunications sectors function as regional leads, it remains to be seen whether the relevant agencies within these two sectors will be able to pull together the level of coordination and resources required to effectively protect and secure CUI.

The concept paper suggested leveraging existing regional maritime domain awareness capabilities, strong information-sharing links and potentially maritime and air assets to contribute to the efforts to address the threats to CUI. In addition, suggestions were made for CUI protection to be woven into the agenda of ADMM-Plus Expert Working Groups on maritime security, cyber security and counter terrorism, and featured in joint training and table-top exercises.

Accelerating the Momentum for Southeast Asia

Owing to the frequency of incidents in their region, the Baltic countries have been at the forefront of developing CUI protection measures. One such measure is the establishment of national centres (such as that in Sweden) to coordinate awareness and responses from the respective economic, energy, telecommunications and security agencies. More important though are the regional cooperation mechanisms that have taken shape among affected governments and industry stakeholders. These are mechanisms that Southeast Asian member states could consider adopting.

The impetus to cooperate is a strong one. The geography of Southeast Asia is such that many submarine cables and pipelines pass through the waters and jurisdictions of neighbouring states. The current gaps in the international legal regimes have led to a general lack of enforcement and adjudicative jurisdiction to protect CUI beyond one's territorial waters. Given the growing urgency of protecting CUI, Southeast Asian member states should consider accelerating the implementation of the measures listed in the ADMM Concept Paper.

Underwater cables are critical yet vulnerable to sabotage, hence the need for stronger and more proactive regional cooperation among ASEAN member states.
Image source: Defense Visual Information Distribution Service.

Starting with Regional Awareness and Information-sharing

The Information Fusion Centre (IFC) was identified in the ADMM Concept Paper as a potential regional reporting hub for incidents affecting CUI. Set up in 2009 in Singapore, the IFC is a multinational maritime-security hub, with strong linkages to both security agencies and the shipping community. In terms of maritime domain awareness, the IFC today monitors commercial ships worldwide and has demonstrated its ability to alert partners to respond when there are maritime incidents. Timely response is possible because of a voluntary reporting network: shipping companies provide real-time updates, allowing the IFC to bridge the gap between an incident and an agency's intervention. Examples include its role in facilitating the rescue of the Singapore-flagged ship *MV Success 9* and in addressing sea robbery incidents in the Singapore Strait.

However, there are more stakeholders for CUI protection as it involves commercial entities from the economic, energy and telecommunications sectors as well. Taking a leaf from the Baltic experience, there needs to be closer partnership with the commercial owners of submarine cables as well as companies that own the ships and

assets for maintenance and repair of damaged cables. The IFC is well placed to assume a broader monitoring role for CUI protection since it is already monitoring the maritime space. It can continue to pick out anomalous vessels such as “dark ships” but would need new processes to cue the security agencies as well as the economic, energy and telecommunications sectors in ASEAN, ensuring timely responses from investigation to repairs.

The vulnerability of CUI means that we need to move beyond conceptual discussions towards practical implementation soon. Protecting CUI will require a collaborative and coordinated approach that strengthens legal frameworks, enhances regional awareness and develops credible response mechanisms. ASEAN already possesses many of the foundational elements needed to advance this agenda; for example, the IFC could, for a start, serve as a regional hub for monitoring submarine cable security. CUI protection has already been endorsed as a key priority in ASEAN. What is required is sustained commitment and closer cooperation among defence establishments, civilian agencies and industry stakeholders to make it happen.

Jane Chan *is Senior Fellow and Coordinator of the Maritime Security Programme at the S. Rajaratnam School of International Studies (RSIS) and* ***Nicholas Lim*** *is a Senior Fellow at RSIS.*

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

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