EIAS@EIAS.ORG

POLICY BRIEF
11/2026



BEYOND MARKET ACCESS: PROTECTING EU COMMERCIAL INTERESTS IN THE MALACCA-SINGAPORE MARITIME SYSTEM.

TRADE AGREEMENTS, OPERATIONAL RESILIENCE AND LITTORAL-LED COOPERATION

ALICE CONSIGLIERE
JUNIOR RESEARCHER
EIAS

EIAS

Beyond Market Access: Protecting EU Commercial Interests In The Malacca-Singapore Maritime System.

Trade agreements, operational resilience and littoral-led cooperation

Abstract

The EU's expanding trade agenda and investment relationships with Singapore, Malaysia and Indonesia depend not only on preferential market access, but also on the operational reliability of the Malacca and Singapore Straits' maritime systems. Disruptions affecting ports, shipping and digital infrastructure can undermine commercial flows even when sea lanes remain legally open. Port cybersecurity, high-risk ship-to-ship (STS) transfers, and delays in submarine-cable repair illustrate how operational weaknesses can translate into higher costs, uncertainty and disruption for European-linked trade. EU trade agreements can improve regulatory predictability and digital-trade conditions, but they cannot address these risks on their own. They should be complemented by targeted cooperation on maritime resilience, information-sharing and implementation with the littoral states, building on existing regional mechanisms rather than duplicating them.

1. The Strategic Importance of Maritime Resilience

As Mr. Jeffrey Siow, the Singaporean Minister for Transport, stated during the 17th Co-operation Forum convened by Indonesia, Malaysia and Singapore on 25-26 August 2026, recent crises in the Red Sea and the Strait of Hormuz have highlighted the vulnerability of key maritime chokepoints and their importance to economic security. It is essential to note that disruptions can occur aside from military blockade, as the operability and functionality of straits depend on many operational and technical factors. This is particularly true for the Straits of Malacca and Singapore (SOMS), forming one of the world's busiest sea lanes, managed by three different littoral states.

The resilience of the Straits of Malacca and Singapore is increasingly crucial for the EU's economic security following the publication of the 'EU's Indo-Pacific Strategy', whose agenda includes deepening its relations with ASEAN states through trade agreements. Therefore, the SOMS are a useful area of study to understand the link and interdependence between market access and a commercial-resilience strategy, in order to make Free Trade Agreements (FTAs) and Comprehensive Economic Partnership Agreements (CEPAs) as operative as possible. Non-military commercial vulnerabilities in the Straits therefore call for the EU to complement its market-access agenda with targeted maritime-resilience cooperation with the littoral states, strengthening economic ties with ASEAN while addressing existing gaps in economic security.

The suggested EU approach is layered. The ASEAN-EU dialogue should therefore provide strategic coordination and promote interoperability, while practical EU engagement should remain case-specific and channeled through existing regional mechanisms, national maritime authorities, private systems and EU technical programmes.

2. Why the Malacca-Singapore System Matters To EU Commercial Interests

The ASEAN region is a dynamic market and ranks as one of the top eight economies in the world. That is why ensuring better access for EU exporters is a priority for the EU. As a bloc, the 11 Southeast Asian countries count as the EU's third-largest trading partner outside Europe, right after the US and China. So far, the EU has concluded bilateral free trade and economic partnership agreements with Singapore, Vietnam and Indonesia, and there are ongoing negotiations with Thailand, the Philippines and Malaysia. As the Centre for

European Reform highlights, bilateral trade exchanges between the EU and ASEAN are the highest of any two regions in the world.

Much of this trade passes through maritime chokepoints in the Indo-Pacific region such as the Malacca and Singapore Straits. In 2024, goods worth more than 2.4 trillion EUR transited the Malacca Strait, equivalent to roughly 21% of global maritime trade and over 10% of global trade. These crucial bottlenecks bring on a critical level of openness obtained through signed and incoming trade agreements. Therefore, through its Indo-Pacific Strategy, the EU stresses how it is essential to ensure cooperation with regional partners and promote the resilience of open, diversified, and undistorted market access. As UNCTAD's Review of Maritime Transport 2025 documents, operational disruptions do not need to take the form of a complete closure to affect commerce. Cyber incidents in ports, uncertainty surrounding STS transfers or a delay in cable repair are recurring features of global shipping, with potential consequences for EU commercial interests in terms of shipping costs, delays and insurance premiums. Market indicators, such as the Drewry World Container Index, illustrate how shipping costs can move rapidly in response to congestion, route disruptions and schedule unreliability.

Consequently, since 2013, the EU has intensified its ties with ASEAN in this domain, through their dialogue on Maritime Security Cooperation and the ASEAN Regional Forum (ARF). The 21st ASEAN Economic Ministers (AEM)-EU Trade Commissioner Consultation of 25 September 2025 identified supply-chain resilience as a shared economic priority for both ASEAN and the EU. It also highlighted the institutional channels through which this cooperation can be pursued, notably the Trade and Investment Work Programme 2026–2027 (TIWP) and SCOPE Trade, which are intended to support work on regional standards, regulatory capacity and more resilient trade relations. Their purpose is to reduce the uncertainty and disruption faced by shippers and logistics providers, helping to ensure that the market access created through trade agreements remains commercially meaningful in practice.

3. Existing Rules and Instruments: Different Functions, Different Instruments

The EU's commercial interests in the Malacca and Singapore Straits depend on a layered governance framework led by the three littoral states and underpinned by UNCLOS and International Maritime Organisation (IMO) rules. Littoral-led mechanisms coordinate

navigation safety and environmental protection, while international maritime law provides the baseline obligations for safe and efficient shipping.

Part III of the UNCLOS regime guarantees the 'right of transit passage', but legal openness does not by itself ensure commercial or operational reliability. Article 43 encourages user states to cooperate on navigational and safety aids with Indonesia, Malaysia and Singapore, while the littoral states retain sovereignty and jurisdiction over their waters. This cooperation requirement was operationalised in 2007 through the IMO-supported Co-operative Mechanism on Safety of Navigation and Environmental Protection in the SOMS, the key platform that brings together littoral states, user states, industry and other stakeholders. At the 17th Co-operation Forum in Singapore in August 2026, the three littoral states reaffirmed their shared commitment to keep the SOMS free, open and safe for international shipping. The governance of the SOMS therefore reflects a balance between open navigation and littoral-state authority. This balance matters to the EU because existing frameworks provide channels for cooperation, but do not automatically resolve implementation or interoperability issues. Another recent political reaffirmation of these principles is the EU Pledge on Maintaining the Integrity of the International Law of the Sea (No Fees/No Tools), announced in October 2026 and formally published in November 2026. For the EU, this provides an additional normative basis for engaging with littoral states on the protection of commercial navigation.

Besides international and regional mechanisms, the EU increasingly seeks tailored bilateral engagement that can reinforce regional norms and build trust. For instance, the trade and partnership agreements the European Commission has signed with the littoral states, such as the FTA with Singapore or the CEPA with Indonesia, can improve market access, customs procedures and conditions for services and digital trade. However, they cannot operate ports, repair cables or enforce maritime rules in the Straits. The relevant question is therefore not whether maritime security is absent from EU trade policy, but where existing arrangements and mechanisms leave implementation and coordination gaps that could affect EU commercial interests.

Recent ASEAN-EU developments provide a political basis for addressing these gaps: ASEAN adopted its Maritime Outlook in 2023, while the EU updated its Maritime Security Strategy. The April 2026 ASEAN-EU Ministerial Statement welcomes EU support for maritime security and maritime domain awareness, to complement ASEAN priorities under the ASEAN Outlook on the Indo-Pacific through existing regional projects.

4. Three Operational Exposures

The following three cases illustrate different forms of EU commercial exposure in the SOMS: port cybersecurity affecting logistics continuity, high-risk STS transfers affecting regulatory predictability, and submarine-cable repair affecting digital connectivity.

4. 1 Port Cybersecurity: Protecting the Continuity of European-linked Logistics

On 9 September 2026, a cybersecurity incident hit Malaysia's Tanjung Pelepas Port's (PTP) terminal operating systems, forcing a shutdown of container operations for several hours and the detour of some container ships coming from European harbours. The PTP is one of the world's busiest container transhipment hubs and part of the SOMS system. Alongside the 2017 Maersk attack and other major port disruptions, this incident highlights the growing cyber threat to container shipping and logistics. Amar More, CEO of Kale Logistics Solutions, describes ports as attractive targets for cyberattacks because they concentrate trade, data, and critical infrastructure. The growing interconnectedness of critical maritime systems implies that disruptions can then cascade across wider supply chains.

Considering the incredible amount of data and operating systems involved in the SOMS system and the number of organized crime groups in the region, its vulnerability multiplies. That is why the EU Straitsecurity Project identifies the Malacca and Singapore Straits as relevant case studies for assessing cyber vulnerabilities affecting ships, ports and interconnected maritime systems. The goal of this EU-funded research program is to highlight how cybersecurity can be linked to a lack of expertise, implementation, and enforcement of regulations. The main findings of the research hint that the International Maritime Organization (IMO) guidelines lack specificity, while port state implementation of maritime cybersecurity standards varies. The research highlights the need for stronger international information-sharing mechanisms. Authorities often struggle to assess cyber threats because maritime companies remain reluctant to disclose incidents due to legal, reputational, and commercial concerns. The essential gap is formed when information sharing remains inadequate, and open-source recorded incidents, accessible through instruments like the Maritime Cyber Attack Database (MCAD), are just the tip of the iceberg. Some alignment between SOMS states on maritime security cooperation exists, but not on cyber threats specifically. The recommendations propose to create a consolidated regional framework built upon existing consolidated cooperation initiatives, reinforce training and shipboard systems, along with introducing an anonymous cyberattack reporting system.

In 2017, the IMO Maritime Safety Committee (MSC) adopted a resolution on Maritime Cyber Risk Management affirming that cyber risk management should be taken into account as part of a ship's overall safety management systems. It was followed the same year by the IMO Facilitation Committee (FAL) Guidelines on Maritime Cyber Risk Management, which were updated in 2022 and revised in 2025. These measures complement the broader maritime security framework established by the International Ship and Port Facility Security (ISPS) Code. Maritime cybersecurity already has an international baseline, but implementation remains uneven, particularly in information sharing and interoperability between national and regional systems.

The Singapore case illustrates how international cybersecurity guidance can be translated into operational tools through cooperation between government, industry and academia. In 2024, the Singapore Shipping Association supported the creation of the MaritimeSG Shipping CyberSafe Scorecard. This voluntary industry-oriented tool was designed to improve cyber-risk maturity across vessel operations, including among smaller operators. It was accompanied by a prototype Maritime Cyber Assurance and Operation Centre (MCAOC), jointly hosted by the Maritime and Port Authority of Singapore (MPA) and industry to support monitoring, information dissemination, and coordinated response and recovery.

Singapore's approach shows that useful cybersecurity instruments already exist, but their value for the wider SOMS depends on their reach and interoperability across ports and authorities. For EU-linked logistics, the main risk is the loss of predictability and continuity at a major transhipment node. The policy challenge is therefore to improve the implementation and cross-jurisdictional interoperability of existing arrangements.

4.2 STS Transfers: Commercial Compliance and Regulatory Predictability

Ship-to-Ship (STS) transfer operations consist of moving cargo such as crude oil, petroleum products or liquefied natural gas from one seagoing vessel to another, either while stationary or underway. STS transfer mechanisms are governed by Chapter 8 of the Convention for the Prevention of Pollution from Ships (MARPOL) Annex I, which prescribes the requirements and rules ships have to follow to ensure the safe development of these operations. The requirements include carrying an STS Operation Plan on board and notifying at least 48 hours in advance if the operation is planned to occur in a Party's territorial sea or exclusive economic zone.

STS transfers are not inherently problematic. The main concern is an opaque or non-compliant activity, which can create safety, environmental, sanctions, insurance, and supply-chain risks for European-linked trade. The IMO Resolution A.1192 (33) calls on stakeholders to strengthen the prevention of illegal operations brought on by what are defined as dark or shadow fleets, which deliberately conceal AIS (Automatic Identification System) or LRIT (Long-Range Identification and Tracking) signals in order to bring on dark STS transfers of oil and disguise cargo origin or ownership. Conducting STS transfers without a valid permit and recognition is no longer viewed by local regulators as a minor, technical administrative oversight. Instead, it is treated as a serious statutory breach. The resolution encourages coastal states to monitor STS operations in their territorial seas and Exclusive Economic Zones (EEZs), while calling on states and industry to strengthen information sharing and due diligence. Compliance risk and regulatory uncertainty where enforcement is weakest are the main exposures the EU should monitor.

On 23 March 2026, the Malaysian Maritime Enforcement Agency (MMEA) detained two oil tankers suspected of conducting unauthorised STS activities near Pulau Jarak. The vessels were suspected of transferring approximately 750 metric tonnes of marine fuel oil without the required permit, while anchoring in an unapproved area. Malaysia's Merchant Shipping Ordinance 1952 establishes a domestic approval and notification framework and empowers the MMEA to detain vessels, initiate formal investigations and pursue criminal prosecution. The case highlights the difficulty of enforcing domestic rules once STS operations move beyond the effective reach of national authorities, particularly in the so-called Outer Port Limits (OPL) areas. In addition, detention can itself generate significant commercial disruption, including delays to cargo operations, interruption of charter-party performance and increased costs. Malaysia has sought to address this gap through the implementation of two new regulatory areas within its 2026 EEZ framework. Located near the eastern approaches to the Traffic Separation Scheme in the SOMS, they extend compliance checks into OPL areas. These new areas represent a partial response to the enforcement challenge: if non-compliant activity can migrate further offshore, the case reinforces the limits of purely national enforcement and the need for stronger cross-jurisdictional monitoring and information-sharing among the littoral states.

Since the SOMS funnel enormous shipping traffic, the waters beyond Singapore's jurisdiction in the Eastern Outside Port Limits (EOPL) can also offer convenient anonymity for dark STS transfers. Singapore has a relatively developed and formalised STS oversight framework, but, as in Malaysia, its main limitation is jurisdictional rather than regulatory. Illegal activities often occur beyond the direct reach of Singapore's port authority controls.

As a result, dark STS transfers involving AIS gaps and spoofing remain difficult to detect and verify.

4.3 Submarine-Cable Repair: Making Digital Trade More Operationally Resilient

Modern financial and digital infrastructure depends heavily on subsea cables, creating concentration risks and resilience vulnerabilities when multiple providers rely on the same physical routes. Around 99% of international digital traffic travels through subsea cables, which also support large volumes of daily financial transactions.

On 23 October 2023, SEA-ME-WE-5 was taken out of service for repair after a shunt fault in the Indonesian waters of the SOMS. The SEA-ME-WE-5 is a 20,000 km cable system linking Southeast Asia with Europe, from Singapore to its landing ports in France and Italy. A shunt fault occurs when seawater breaches the cable's insulation, causing a short circuit in the cable's electrical feed. The fault disrupted traffic between Singapore and Bangladesh, reportedly reducing Bangladesh's internet capacity by approximately one-third. The case illustrates how Indonesian protectionist cabotage requirements extended initial repair timelines from days to several weeks, with repairs continuing into late May 2024.

These dynamics echo the broader findings of previous EIAS analysis on European cable security, and show that a technical fault in one section of a Europe-Asia cable system can become a commercial problem for EU-linked digital trade when repair capacity, spare parts and authorisation procedures do not align. The European Commission's Report on Security and Resilience of EU Submarine Cable Infrastructures identifies long repair-permit processes and jurisdictional limits in the EEZs and the high seas as key dependencies. Around 200 subsea cable faults occur each year, while repairs depend on a limited and ageing global fleet of specialist vessels. As a result, even when a reliable failover path exists, increased latency can degrade service quality and increase operational costs. In addition, in its risk scenarios, the report explicitly considers a scenario in which cable damage in a third country's waters affects multiple EU Member States, noting that cross-border coordination can increase recovery costs and complexity. Finally, the European Commission's Expert Group on B2B Data Sharing and Cloud Computing Report of 2025 also observes that some Asian regions can have more complex and time-consuming permitting procedures.

According to existing EIAS analysis, no ASEAN state currently possesses sovereign repair capabilities. Regulatory ambiguities and fragmented permitting arrangements can undermine the resilience of undersea cable infrastructure. In the Indo-Pacific, where cables

cross multiple jurisdictions, administrative paperwork can delay both repairs and construction. ASEAN has sought to address these challenges through the Enhanced ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables, adopted in January 2026. They encourage ASEAN member states to designate a single coordinating authority, provide pre-clearance for repair vessels and crews, and exchange information on cable incidents to identify protection and repair gaps. These guidelines provide a clear regional basis for the EU's engagement. The EU should monitor their implementation and, where requested, support regulatory streamlining and faster repair authorizations through existing ASEAN-EU dialogue, technical cooperation and digital-connectivity channels. Altogether, these three cases suggest that the main challenge for the EU is not the absence of relevant arrangements, but gaps in their implementation and coordination. They also show that EU commercial exposure in the SOMS is more likely to arise from the accumulation of operational vulnerabilities across ports, digital infrastructure and shipping practices than from a single catastrophic disruption.

5. The EU's Response: Matching Instruments to Vulnerabilities

Protecting EU commercial interests in the SOMS requires a more targeted use of existing instruments, aligned with the specific vulnerabilities identified above and the sovereign sensibilities of the littoral states. The April 2026 ASEAN-EU Joint Ministerial Statement provides a recent political framework for this approach as the parties call critical maritime infrastructure resilience vital and welcome EU support for maritime security and maritime-domain awareness through technical cooperation, capacity-building and exchanges. The EU is already providing extensive technical assistance and capacity building around the world, including the ASEAN region, but its activities could be much more tailored to the needs of businesses and operators on the ground. This document sets the political and operational conditions for EU action and brings out some already existing EU programmes, such as CRIMARIO and ESIWA+, which could be used as supporting mechanisms to cover the previously mentioned vulnerabilities.

5.1 Trade and Regulatory Instruments

For commercial operators, regulatory predictability depends on the knowledge and awareness of which procedures apply and which authority to contact. The EU should use its trade and regulatory dialogues to seek greater clarity on these points, particularly where

administrative requirements delay maritime services or cable repairs. Operational response, however, remains a task for the competent authorities and operators.

At the regional level, the ASEAN-EU Trade and Investment Work Programme (TIWP) and the Joint Working Group on Trade and Investment (JWG) provide channels for supply-chain resilience and regulatory cooperation. Specifically, if a problem concerns topics such as regional standards and regulatory capacity, the EU does not necessarily need to insert it into each bilateral FTA, it can first pursue it through the TIWP.

Improving access for EU exporters to the ASEAN market remains an EU priority. However, as highlighted in the EU-ASEAN White Paper, trade facilitation also depends on robust risk-management and enforcement mechanisms. FTAs offer the EU and ASEAN an opportunity to strengthen regulatory cooperation across the region. The EU promotes high standards of transparency and good regulatory practice, while ASEAN has also strengthened its commitment to regulatory transparency in recent years, particularly in trade-related measures, although implementation remains uneven. Yet, altogether, bilateral agreements can support transparency, customs cooperation, services access and digital-trade conditions.

The EU and Singapore signed a digital trade agreement (EUSDTA) in 2025, which is already in force, with the aim of keeping pace with the fast-evolving nature of the digital economy. The agreement can support broader cooperation on trusted digital commerce and the exchange of information to identify and mitigate cybersecurity threats. However, addressing practical maritime-cyber cooperation requires the involvement of port authorities and technical and private partners. Furthermore, a significant recent development is the signature of the EU-Indonesia Comprehensive Economic Partnership Agreement (CEPA) and Investment Protection Agreement (IPA) on 21 November 2026. These agreements include Indonesia's commitment to refraining from imposing import volume controls, easing pre-shipment inspection requirements, and providing preferential treatment on export duties. In January 2025, the EU and Malaysia announced the resumption of negotiations for a comprehensive and modern Free Trade Agreement (FTA), for which the sixth round is scheduled for the beginning of 2027. Through these talks, the EU could push enhanced transparency and customs cooperation to boost a predictable treatment of maritime and digital service providers. FTA and CEPA negotiations should incorporate maritime operability from the outset. However, meaningful maritime and digital resilience requires complementary instruments that address the operational conditions on which increased trade depends.

5.2 Maritime Information-Sharing and Interoperability

Maritime information-sharing and interoperability instruments are most relevant to address coordination problems, including helping authorities exchange relevant vessel-risk information across jurisdictions. Their limitation, however, is that they cannot resolve political sensitivities over data-sharing or replace the legal authority of littoral states.

CRIMARIO (Critical Maritime Routes in the Indian Ocean) is the practical EU instrument for inter-agency coordination and incident management, providing technical support and information-sharing capacity on maritime capacity where requested. Its most relevant output is IORIS (the Indo-Pacific Regional Information Sharing Platform), a neutral, secure platform that enables participating national agencies and regional partners to share information, coordinate, and manage incidents voluntarily. For Singapore, IORIS should complement existing maritime information-sharing and incident-management systems by facilitating communication between port authorities, operators, and technical partners during cyber incidents. In the STS context, it could support the exchange of vessel-risk information and strengthen AIS-enabled awareness and identification of competent authorities. At the fourth IORIS Steering Committee Meeting in Mombasa in June 2026, the use of the platform was discussed for shipping security, port safety, and dark fleet monitoring. In the same month, IORIS reported supporting a boarding operation through real-time vessel monitoring. These examples demonstrate its potential for incident communication and inter-agency coordination in the STS field. Finally, it could support further coordination between authorities and operators in the submarine-cable context by presenting IORIS as optional interfaces or supplementary tools to Indonesia and regional ones.

Any EU proposal should respect littoral states' preference for sovereign and ASEAN-centred mechanisms. Indonesia and Malaysia have participated in some IORIS-linked activities but are not formal members, while Singapore maintains its own information-sharing arrangements, including the Information Fusion Centre. A further advancement is the establishment of the ASEAN Maritime Centre in the Philippines in November 2026, which aims to facilitate information-sharing, research and cooperation across maritime-related initiatives. The EU should therefore explore ways to complement this emerging framework and focus on interoperability, rather than introducing parallel structures.

The problem of fragmented maritime governance and insufficient interoperability under conditions of sovereignty sensitivity could be bypassed with the SHARE.IT platform, still included in the CRIMARIO program and developed with the United Nations Office on Drugs

and Crime (UNODC). This tool is not primarily a maritime-information platform, but an interoperability framework designed to connect existing sovereign information-exchange systems securely, allowing selected information to move between different maritime centres without requiring them to replace their own system. In January 2023, the second SHARE.IT Interoperability Framework Conference included the Singapore Information Fusion Centre, demonstrating how this tool has effectively been tested in the SOMS system through a prototype connecting information-exchange systems for a simulated container-vessel drug-trafficking scenario.

5.3 Security-cooperation and Capacity-building Instruments

Security-cooperation and capacity-building instruments should be primarily used to address preparedness problems: supporting partner-requested work on port incident communication, cyber resilience and preparedness. Before a port cyber incident occurs, authorities, operators and technical teams need to establish who will communicate, who will coordinate the response and how recovery will be organised. What these instruments cannot address are structural capacity constraints, as well as determining national security priorities or replacing littoral-led governance.

One of the most concrete tools is ESIWA+, an EU-funded programme to enhance security cooperation in and with Asia and the Indo-Pacific that runs from October 2024 to September 2027. This could play an important role in the context of port cybersecurity for exchanges on incident-response responsibilities and recovery preparedness or by organizing tabletop exercises on communication during a port cyber incident. Furthermore, clear evidence has been found of ESIWA+ supporting cooperation on submarine-cable security. In September 2025, an ESIWA+ supported EU-Vietnam roundtable examined maritime threats and cable protection and discussed critical-infrastructure resilience and incident response.

Building cyber capacity could also be addressed through EUCyberNet II, a relevant tool for exchanges of expertise, training and regional cooperation. In addition, the second phase of this EU-funded project (2025-2028) dedicates particular attention to the Indo-Pacific, especially to Malaysia and Indonesia, and covers cyber legislation and strategies. For instance, by strengthening the Computer Security Incident Response Teams (CSIRTs) and cooperation with stakeholders.

6. Connecting Existing Systems: An EU Approach to Maritime Resilience

The Malacca-Singapore Straits show that market access alone does not guarantee commercial reliability. Trade agreements can open markets and reduce tariffs, but their commercial value depends on whether ports, shipping practices and digital infrastructure can absorb increased trade reliably. As the three cases illustrate, the main challenge lies not necessarily in the absence of relevant instruments, but in their fragmented implementation and limited interoperability, both across different national systems and public and private ones.

The EU should therefore place interoperability at the centre of its approach to maritime resilience. European engagement should focus on connecting existing national and private systems through platforms that offer practical opportunities to facilitate information exchange and coordination, such as IORIS and SHARE.IT. This approach would avoid the duplication of already existing systems, while allowing littoral states to retain sovereignty over them.

An EU trade agenda that incorporates this maritime resilience dimension would strengthen resilience overall while providing more reliable conditions for European businesses operating across the region.



IMAGE SOURCE: HTTPS://PIXABAY.COM/PHOTOS/SHIP-CONTAINER-SHIP-TRACTOR-6794508/

European Institute for Asian Studies - EIAS a.s.b.l.

26 Rue de la Loi, 10th floor
B-1040 Brussels

Tel.: +32 2 230 81 22
E-mail:eias@eias.org
website: www.eias.org

LinkedIn: European Institute for Asian Studies
Facebook: EiasBrussels
Twitter: @EIASBrussels

EIAS