The Hague Centre
for Strategic Studies

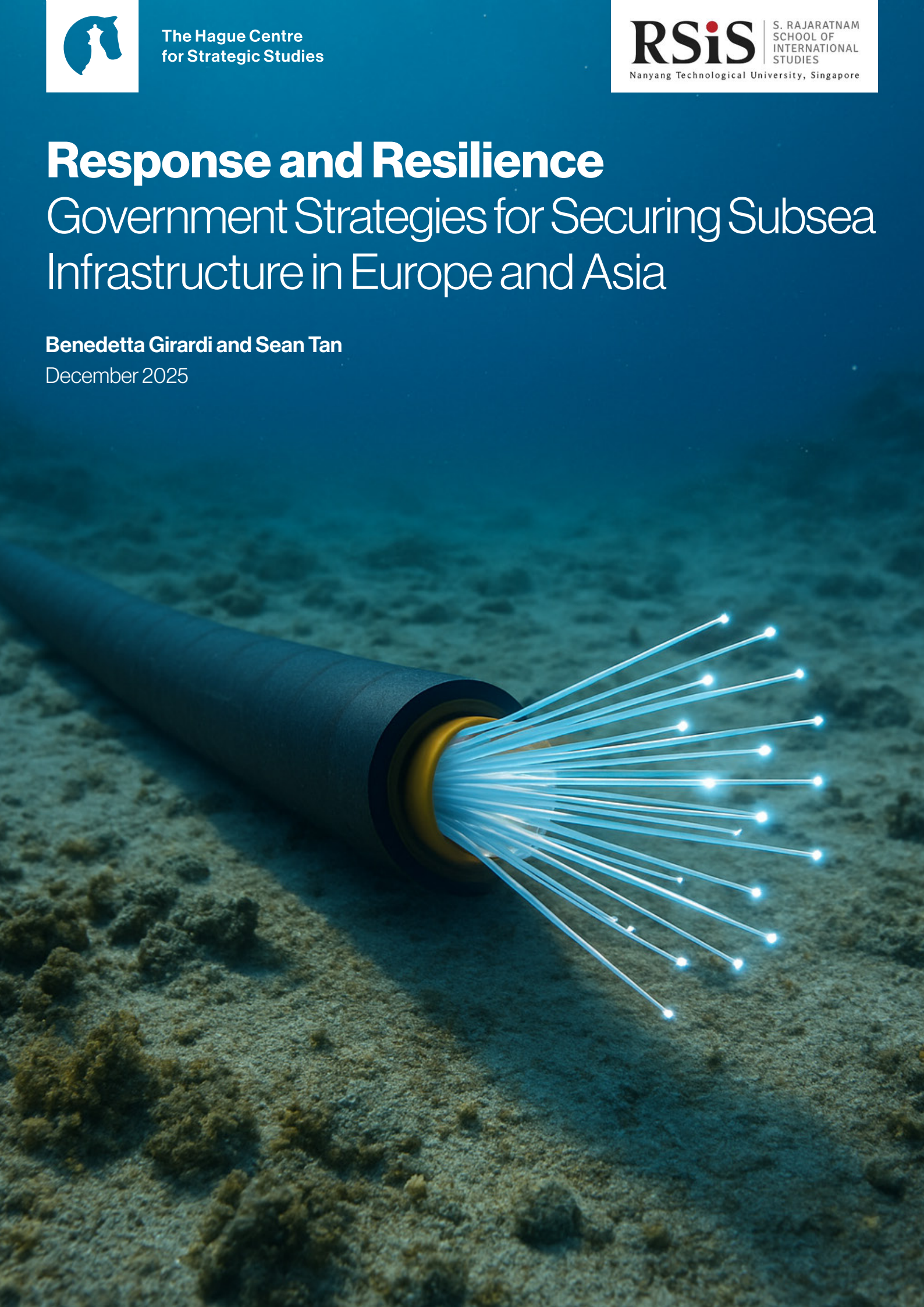
RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Response and Resilience

Government Strategies for Securing Subsea Infrastructure in Europe and Asia

Benedetta Girardi and Sean Tan

December 2025



The Hague Centre
for Strategic Studies

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

Response and Resilience

Government Strategies for Securing Subsea Infrastructure in Europe and Asia

Key Findings Expert Workshop Singapore 30 October
Joint Paper by HCSS & RSIS

Authors:
Benedetta Girardi and Sean Tan

Quality assurance:
Tim Sweijs and Benjamin Ang

Cover source:
AI-generated

December 2025

The research for and production of this paper has been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

The report is the result of a collaboration between HCSS in cooperation with RSIS and The Embassy of the Kingdom of the Netherlands in Singapore.

Table of Contents

Introduction

As highly connected and technologically advanced nations, Singapore and the Netherlands serve as critical hubs in global financial, trading, and communications networks. Their prosperity and security depend on the uninterrupted operation of critical undersea infrastructure (CUI), including internet cables, energy pipelines, and power lines that traverse the seabed. However, this infrastructure faces growing risks from both accidental damage and deliberate hostile actions.

Both countries share a high degree of exposure due to their dense populations, reliance on global data flows, and integration into international supply chains. Yet, their strategic environments differ: Singapore sits at the crossroads of the Indo-Pacific's contested sea lanes, while the Netherlands anchors Europe's North Sea network at the heart of transatlantic connectivity. Despite these differences, both nations confront similar challenges in protecting their CUI from espionage, sabotage, and disruption amid rising hybrid threats.

To safeguard their national interests, Singapore and the Netherlands must strengthen resilience, enhance deterrence by denial, and develop means to impose costs on hostile actors. This requires coordinated investment in research and development (R&D) and research and technology (R&T), greater industry–government collaboration, and sustained political engagement. By sharing lessons learned and exploring joint initiatives, the two nations can build more secure and adaptive systems capable of withstanding the evolving threat landscape beneath the seas.

This report explores the threats, policy responses, and challenges that Singapore and the Netherlands face in addressing CUI vulnerabilities. In Part 1, the report looks at the current state of affairs. More precisely, it delves into the CUI threat landscapes in Asia and Europe and analyses how Singaporean and Dutch governments have so far responded to such threats. It also looks at the common challenges and policy gaps that still persist. Part 2 takes the analysis a step further by identifying key steps necessary to enhance prevention and enforcement. On the basis of this, Part 2 also lays the foundations for a comprehensive Singapore-Netherlands agenda by looking at the cooperation venues available to the two states. Lastly, the findings are summarised in the conclusion.

Part 1.
The state of affairs: the current CUI threat landscape and government responses

1.1. Setting the scene: strategic infrastructure at risk

This section analyses the evolving risk environment facing CUI with particular emphasis on human-created threats. It explores how accidental damage, cyberattacks, and suspected acts of sabotage have become increasingly significant drivers of vulnerability across global seabed networks. The discussion situates these risks within the broader geopolitical and economic contexts of Europe and Asia, where heightened strategic competition and hybrid operations have amplified the exposure of CUI to deliberate interference. Indeed while around 12% of cable cuts are caused by natural hazards, accidental cable faults, and more precisely fishing and anchoring activities concern over 70% of global cable cuts. Grey zone activities like sabotage, which can be considered as piracy under UNCLOS 100/101 and violates UNCLOS 113, are the third largest cause for global cable cuts.[1] By examining both the patterns and root causes of such threats, this section seeks to clarify the interplay between human activity, technological dependency, and state behaviour, laying the groundwork for assessing the adequacy of existing countermeasures in subsequent sections.

1.1.1. Key threat vectors to CUI

As CUI in Europe faces increasing risks, three primary threat vectors have emerged, each posing distinct challenges:

1. **Grey zone activities**: These covert actions, often difficult to attribute, aim to disrupt infrastructure without provoking direct conflict. Examples include the damage of the EstLink2 power cable and other four telecommunications cables (2024) and repeated cable strikes in Dutch and UK sectors (2019–2024), exploiting the ambiguity between peace and war.[2]
2. **Military activities**: Direct state-led attacks on subsea infrastructure can have significant strategic consequences.[3] The Nord Stream pipeline explosion (2022) is a prime example

---

1 International cable Protection Committeee, 'Publications of theICPC', ICPC, 8 May 2025, https://www.iscpc.org/publications/.

2 Frank Bekkers et al., *The High Value of The North Sea* (The Hague Centre for Strategic Studies, 2021), 1–100, https://hcss.nl/wp-content/uploads/2021/10/Value-of-the-North-Sea-HR.pdf; Henri van Soest et al., *Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience* (2025), https://www.rand.org/pubs/perspectives/PEA3800-1.html.

3 Bekkers et al., *The High Value of The North Sea*; van Soest et al., *Evolving Threats to Critical Undersea Infrastructure*.

of military operations targeting vital energy networks to achieve geopolitical objectives, with broader implications for regional security.

3. **Accidental instances**: Unintended damage, such as anchor drag of fishing vessels in or damage incurred during the installation of undersea cables, underscores the risks from human error and operational failures, which can disrupt critical infrastructure and services.[4]

Table 1 below offers an overview of the three threat vectors and the underlying threat types that have recently been observed in Europe as disruptors to CUI.

Table 1: summary of threat vectors, types, and examples occurred in Europe

Category	Threat Type	Description	Infrastructure Targeted	Examples
Grey Zone Activities	***Sabotage***	Covert actions aimed at damaging or obstructing infrastructure for political or military gain during peacetime.	*Telecommunications cables, pipelines*	• *Estlink 2 and telecommunications cables (2024)* • *Unexplained subsea cable damages near Shetland Islands and Norway (2023)* • *Yi Peng 3 potentially responsible for cutting two undersea cables on her journey through the Baltic Sea (2024)* • *Trans Pacific Express cable system suspected attribution to Xingshun 39 (2025)*
	Cyber Operations	Covert interference with ICT systems connected to maritime infrastructure.	*Telecommunications cables, gas pipelines*	• *Ransomware incidents affecting offshore wind control systems in Northern Europe (2020-2024)*
	Incursions	Grey zone tactics by military vessels that violate the sovereignty of coastal states or test their defences.	*Telecommunications cables, pipelines*	• *Loften-Vesterålen Ocean Observatory (2021)* • *Svalbard Undersea Cable System (2022)* • *Repeated cable strikes from trawlers in the Dutch and UK sectors (2019–2024)* • *Matsu Islands (Taiwan) cable cuts from Chinese vessels in February 2023*
Military Activities	***Physical Attacks***	Military operations targeting maritime assets, including submarines or UUVs to damage undersea cables, pipelines, and monitoring systems.	*Telecommunications cables, pipelines, surveillance systems*	• *Loften-Vesterålen Ocean Observatory (2021)* • *Nord Stream pipeline explosions (2022) in the Baltic Sea*
	Cyber and Electromagnetic Activities	Military operations aimed at compromising ICT systems, such as cyberattacks or electromagnetic pulse attacks on CUI.	*Telecommunications cables, gas pipelines*	• *Svalbard Undersea Cable System (2022)*
	Espionage	Intelligence-gathering military operations, including tapping undersea cables or deploying sensors to access communications.	*Telecommunications cables*	• *Balticconnector (2023)* • *Russian vessel "Yantar" and other survey ships observed near European cable routes (2017–2023)*
Accidental Damage	***Anchor Dragging / Physical Damage***	Damage to subsea infrastructure caused by large vessels or anchors.	*Telecommunications cables, gas pipelines*	• *Ship dragging its anchor on the seabed in the English Channel cut the three main internet cables to the Channel Islands (2016)* • *Damages to the AAG submarine cables in Vietnam (3-5 times per year between 2017-2021)*
	Operational Errors	Disruptions caused by errors in the configuration or operation of infrastructure.	*Telecommunications cables, offshore wind farms*	• *Configuration error in Dutch offshore interconnector system (2019) caused short outage* • *Malfunctioning of Vietnam's APG undersea Cable after reparations (June 2023)*

[4] International Marine Contractors Association (IMCA), 'Unravelling Subsea Cable Failure in Offshore Wind', accessed 22 October 2025, https://www.imca-int.com/news-events/commentary/unravelling-subsea-cable-failure-in-offshore-wind/; Bekkers et al., *The High Value of The North Sea*.

1.1.2. The threat landscape in Europe/the Netherlands

1.1.2.1. Context and strategic importance

Europe's prosperity and security depend heavily on an extensive network of subsea communication cables, pipelines, and energy interconnectors that sustain its digital economy and energy transition. The Baltic and North Sea, in particular, have become critical hubs for both global data transmission and offshore energy production. They host a dense concentration of internet cable landing points, offshore wind farms, and energy pipelines linking the United Kingdom, the Netherlands, Germany, and Scandinavia. This concentration makes the region one of the most interconnected yet vulnerable maritime spaces in the world.[5]

For the Netherlands, this strategic importance is amplified by its role as both a gateway to Europe and a core node in global data flows. The Dutch coastline hosts several major subsea cable landing stations and serves as a logistical and digital hub connecting North America and Europe. The Port of Rotterdam, Europe's largest, underscores the Netherlands' role in critical maritime trade and energy transit. As a result, disruptions to CUI, whether from physical tampering, cyber-attack, or accidental damage, could have cascading consequences for European connectivity, financial stability, and energy security. The Netherlands' integration into EU and NATO networks also ties its infrastructure protection directly to broader regional security concerns, making the resilience of Dutch CUI a matter of collective European and transatlantic interest.[6]

1.1.2.2. Drivers and root causes

The increasing threats to CUI in Europe stem from a complex interplay of geopolitical, technological, and economic factors. These dynamics have transformed the maritime domain into a contested strategic environment, where both state and non-state actors exploit vulnerabilities in vital undersea systems.

1. **Expansion of sea-based economy and economic dependencies**: The growing reliance on maritime trade and energy infrastructure in Europe has made undersea assets more vulnerable, as they are key points of access for economic activities and supply chains.[7]
2. **Geopolitical competition and strategic rivalries**: Heightened geopolitical tensions, particularly in the North Sea region, fuel competition for control of critical infrastructure, leading to increased risks from state and non-state actors.[8]
3. **Conflict in Ukraine and regional security disruptions**: The ongoing conflict in Ukraine has intensified regional security concerns, particularly regarding energy supply lines and infrastructure. The provision of aid to Ukraine also depends on functioning CUI.[9]
4. **Advancements in technology**: The convergence of cutting-edge technologies such as robotics, sensors, AI, and autonomous systems has significantly enhanced the ability to damage or disrupt CUI. These technologies, once the domain of powerful state actors, are now increasingly accessible to smaller states, criminal groups, and terrorist organisations.[10]

---

5 Jeroen de Jonge and Casper Bosschaart, *Protecting Our Critical Undersea Infrastructure Together* (TNO, 2025); Bekkers et al., *The High Value of The North Sea*.

6 Bekkers et al., *The High Value of The North Sea*; 'Dutch Authorities Enhance Surveillance amid Russian Vessel Activity in European Waters | NL Times', 23 January 2025, https://nltimes.nl/2025/01/23/dutch-authorities-enhance-surveillance-amid-russian-vessel-activity-european-waters.

7 Bekkers et al., *The High Value of The North Sea*.

8 Bekkers et al., *The High Value of The North Sea*.

9 de Jonge and Bosschaart, *Protecting Our Critical Undersea Infrastructure Together*.

10 Henri van Soest, *Protecting Europe's Critical Undersea Infrastructure Depends on Coordination and Collaboration* (2025), https://www.rand.org/pubs/commentary/2025/06/protecting-europes-critical-undersea-infrastructure.html.

1.1.2.3. Implications for the Netherlands

The Dutch North Sea hosts 3,600 km² of shipping routes, ~160 oil and gas platforms, 4,000 km of subsea cables and 2,500-4,500 km of pipelines:[11] increasing threats to CUI pose significant risks to national energy supply, data connectivity, maritime safety and environmental monitoring. As the Netherlands expands its offshore activities and increasingly relies on undersea infrastructure, the tensions between economic expansion and need for strategic protection of CUI will increasingly intensify. The increasing presence of new actors and technologies in the North Sea, combined with the remoteness of CUI, make CUI protection challenging for an actor with limited naval capabilities such as the Netherlands. The Netherlands hence will increasingly rely on international cooperation for CUI protection.

1.1.3. Current initiatives to counter CUI threats in the Netherlands

The Netherlands, recognising the danger of the threat abovementioned, has a number of ongoing initiatives to strengthen CUI protection. The Netherlands puts a central focus on improving and enhancing intelligence, surveillance and reconnaissance (ISR) to develop detection and deterrence capacities against suspicious activities or hostile presence, before any damage can occur.[12] These ISR capabilities provide continuous situational awareness to protect critical seabed assets. They are also enhanced by the Netherlands' focus on improving infrastructure monitoring and rapid response measures.[13] The state's rapid detection and repair capacities minimize downtime and economic disruption in the Netherlands in a case of sabotage or accident, therefore maintaining energy and data continuity even under hybrid and physical threat conditions. The Netherlands also encourages public-private partnership and coordination of CUI. Coordinated planning and information-sharing which includes privately owned infrastructures leads to more effective protection. Public-private partnerships also permit the state to align national security priorities with its actual operational capabilities ensuring a unified response during incidents. Finally, the Netherlands' integration of regulatory and risk management frameworks relating to CUI enables fast decision-making processes and clear responsibilities, enforcing robust security standards across operators in addition to strengthening Dutch resilience through the integration of cybersecurity, physical safety and environmental protection within national and EU-wide policies. They are mainly carried out at the national level, or internationally with other European countries and within NATO.

1.1.3.1. National initiatives

As part of this multi-layered strategy, the Dutch government started investment in surveillance, detection, and attribution technologies for subsea infrastructure at the national level. These investments, totalling around €250 million, have been mainly carried out under the North Sea Infrastructure Protection Programme (Programma Bescherming Noordzee Infrastructuur, PBNI), started in 2023.[14] The Ministry of Infrastructure and Water Management

---

11 'Diving into Seabed Security | TNO', Tno.Nl/En, accessed 22 October 2025, https://www.tno.nl/en/diving-seabed-security/.

12 Rijkswaterstaat, 'Programma Bescherming Noordzee Infrastructuur', Noordzeeloket, Rijkswaterstaat, accessed 20 October 2025, https://noordzeeloket.nl/functies-gebruik/kabels-leidingen/pbni/; Rudy Ruitenberg, 'Netherlands to Boost North Sea Surveillance to Deter Seabed Threats', Defense News, 20 December 2023, https://www.defensenews.com/naval/2023/12/20/netherlands-to-boost-north-sea-surveillance-to-deter-seabed-threats/.

13 Rijkswaterstaat, 'Programma Bescherming Noordzee Infrastructuur'; Ruitenberg, 'Netherlands to Boost North Sea Surveillance to Deter Seabed Threats'.

14 Rijkswaterstaat, 'Programma Bescherming Noordzee Infrastructuur'; Ruitenberg, 'Netherlands to Boost North Sea Surveillance to Deter Seabed Threats'.

coordinates this program and works together with the Ministry of Defence, the Ministry of Economic Affairs, the Ministry of Climate and Green Growth, the Ministry of Justice and Security, and the Ministry of Foreign Affairs.[15] As part of the programme drilling rills and wind farms are being equipped with tracking systems alongside enhanced satellite capacity. It also supports the deployment of small, crewed vessels designed to monitor underwater activity.[16]

The Ministry of Infrastructure and Water Management also released the Action Plan Strategy to Protect the North Sea, which focuses on strengthening the protection of critical infrastructure in the North Sea between 2024 and 2025. It centres on five key areas: clear governance, improved detection and assessment of threats, enhanced resilience, effective crisis management, and increased cooperation with public and private partners, including other North Sea countries and allies.[17] The Coast Guard and the Royal Netherlands Navy monitor traffic in the North Sea to detect suspicious activities more quickly. Suspicious ships from non-allied countries or non-NATO members are also escorted to prevent any intentional damage to infrastructures.[18]

Under the interdepartmental cooperation of the Protection of North Sea Infrastructure (Bescherming Noordzee Infrastructuur) program, led by the Ministry of Infrastructure and Water Management, the Dutch government also cooperates with the private sector. For instance, the Ministry of Defence cooperated with Dutch company Fugro to collected data and images of CUI in the North Sea for monitoring purposes.[19] Together, these initiatives ensure that the Netherlands commit, at the national level, to a multi-layered strategy on the protection of CUI.

1.1.3.2. **International initiatives**

The Dutch Ministry of Defence is actively involved in protecting underwater infrastructure at the international level through initiatives like the Seabed Security Experimentation Centre (SeaSEC). SeaSEC is a collaboration among six Northern European countries which aims to develop technologies for safeguarding undersea infrastructure.[20] The Netherlands are also involved in NorthSeal, a new maritime security platform launched in January 2025 by six North Sea states (Belgium, the Netherlands, Germany, Norway, Denmark, and the UK) to coordinate surveillance and protect critical offshore infrastructure. The Netherlands is one of its founding members, contributing intelligence and naval assets for monitoring threats such as sabotage and espionage in the Dutch sector of the North Sea.[21] At the EU level, the Netherlands also participate in MARSEC EU, an EU-level annual maritime security exercise designed to test cooperation between EU Member States, agencies, and naval forces in responding to maritime threats. The Netherlands actively participated in the 2024 edition,

15 Rijkswaterstaat, 'Programma Bescherming Noordzee Infrastructuur'; Ruitenberg, 'Netherlands to Boost North Sea Surveillance to Deter Seabed Threats'.

16 Rijkswaterstaat, 'Programma Bescherming Noordzee Infrastructuur'; Ruitenberg, 'Netherlands to Boost North Sea Surveillance to Deter Seabed Threats'.

17 'Beschermen infrastructuur Noordzee, zoals gasleidingen en data- en elektriciteitskabels - Dreiging in Nederland - Rijksoverheid.nl', onderwerp, Ministerie van Algemene Zaken, Ministerie van Algemene Zaken, 18 April 2025, https://www.rijksoverheid.nl/onderwerpen/dreiging-in-nederland/beschermen-infrastructuur-noordzee.

18 Ministerie van Algemene Zaken, 'Beschermen infrastructuur Noordzee, zoals gasleidingen en data- en elektriciteitskabels - Dreiging in Nederland - Rijksoverheid.nl'.

19 Ministerie van Defensie, 'Defensie brengt met civiele technologie onderzeese infrastructuur in beeld - Nieuwsbericht - Defensie.nl', nieuwsbericht, Ministerie van Defensie, 28 January 2025, https://www.defensie.nl/actueel/nieuws/2025/01/28/defensie-brengt-met-civiele-technologie-onderzeese-infrastructuur-in-beeld.

20 Mariska Buitendijk, *Dutch Navy Monitors North Sea Infrastructure with Minehunter*, 5 December 2023, https://swzmaritime.nl/news/2023/12/05/dutch-navy-monitors-north-sea-infrastructure-with-minehunter/.

21 Flanders News Service, 'New Security Platform Operational in the North Sea', Belganewsagency.Eu, 28 January 2025, https://www.belganewsagency.eu/new-security-platform-operational-in-the-north-sea.

held off Cartagena, Spain, alongside six other Member States, focusing CUI protection and illegal maritime activity.[22]

Lastly, as a member of NATO, the Netherlands cooperate closely with the NATO-accredited MARSEC COE in Istanbul to develop doctrine, research, and training on maritime security and hybrid threats. Dutch diplomats and military representatives visited in 2025 to explore joint work on maritime-infrastructure protection.[23] They also support Baltic Sentry, an initiative launched by NATO in January 2025, to strengthen maritime and undersea-infrastructure monitoring in the Baltic Sea. Although focused on Baltic states, the Netherlands supports the mission through NATO's Standing Naval Forces and shared intelligence systems.[24] Finally, the Netherlands closely cooperates with its neighbours with the Joint Declaration on North Sea Infrastructure Protection signed in April 2024 by Belgium, the Netherlands, Germany, Norway, Denmark, and the UK, which commits the six nations to closer cooperation on protecting CUI.[25]

1.1.4. The threat landscape in Asia/Singapore

1.1.4.1. Context and strategic importance

Asia's economic growth and digital connectivity depend heavily on an extensive network of undersea communication cables, energy pipelines, and subsea power links. The Strait of Malacca, the South China Sea, and surrounding maritime zones have become key arteries for global internet traffic and regional energy trade. Connectivity in the Indo-Pacific, a region marked by both economic dynamism and strategic importance, is heavily reliant on these cables.[26]

Singapore, situated at the crossroads of the Indian and Pacific Oceans, hosts one of the world's densest clusters of submarine cable landing points, linking Asia to Europe, the Middle East, and the United States. As of 2023, Singapore hosted 26 active submarine cable systems and seven cable landing stations.[27] This concentration makes Singapore both a critical digital and energy hub and a potential point of vulnerability. Disruptions could have far-reaching consequences for regional data flows, financial markets, and maritime trade. An estimated 99 per cent of Singapore's internet traffic travels through these cables, underscoring their criticality for financial transactions and government operations.[28] As a result, the resilience of Singapore's underwater infrastructure is central not only to its own security but also to the stability of Southeast Asia's interconnected economies.[29]

---

22 'MARSEC EU 24: EU Agencies and Member States Take Part in Live Maritime Security Exercise | EEAS', accessed 22 October 2025, https://www.eeas.europa.eu/eeas/marsec-eu-24-eu-agencies-and-member-states-take-part-live-maritime-security-exercise_en.

23 administrator, 'MARSEC COE – NATO Maritime Security Centre of Excellence', MARSEC COE, accessed 22 October 2025, https://www.marseccoe.org/.

24 'NATO Launches "Baltic Sentry" to Increase CI Security', European Commission, 15 June 2025, https://ec.europa.eu/newsroom/cipr/items/888102/.

25 Claudia Chiappa, '6 Countries Move to Protect the North Sea from Russians', POLITICO, 9 April 2024, https://www.politico.eu/article/6-european-countries-sign-pact-protect-critical-energy-infrastructure-north-sea-from-russia/.

26 Jihoon Yu, 'Securing Submarine Cables: A Critical Imperative for Indo-Pacific Stability', 20 July 2024, https://thediplomat.com/2024/07/securing-submarine-cables-a-critical-imperative-for-indo-pacific-stability/.

27 Robert Beckman, Asha Hemrajani, Tara Davenport, and Sean Tan, *ENHANCING THE SECURITY of SINGAPORE'S SUBMARINE CABLES: STRENGTHS, CHALLENGES, AND OPPORTUNITIES*, (RSIS, 2024), https://cil.nus.edu.sg/wp-content/uploads/2024/07/PR240521_Enhancing-the-Security-of-Singapores-Submaring-Cables.pdf.

28 Ibid.

29 Erin L. Murphy and Thomas Bryja, *The Strategic Future of Subsea Cables: Singapore Case Study* (CSIS, 2025), https://www.csis.org/analysis/strategic-future-subsea-cables-singapore-case-study.

Moreover, the cables that connect Singapore and the wider Indo-Pacific traverse several maritime chokepoints (including the Strait of Malacca and the South China Sea), where heavy maritime traffic and competing territorial claims create complex risk conditions.[30] These physical vulnerabilities are compounded by exposure at the "dry plants" of the cable network (i.e., landing stations and data centres) where network management and terminal equipment are concentrated. Even though modern cables made of optical fibre are highly resistant to interception, cyber intrusions and physical tampering at these nodes remain pressing concerns.[31]

1.1.4.2. Drivers and root causes

1. **Intensifying geopolitical competition:** strategic rivalries in the South China Sea increase risks of interference and surveillance targeting underwater systems. Dense maritime geography and overlapping territorial claims add uncertainty over jurisdiction. Some Southeast Asian states maintain overlapping Exclusive Economic Zones (EEZs).[32] Disputes may hinder incident responses and complicate enforcement against vessels that cause damage.
2. **Concentration of maritime actors:** the Indo-Pacific area is vast, with many state and non-state actors operating in the maritime domain, raising the likelihood of accidental damage. Although Southeast Asia has not experienced state-on-state sabotage of subsea infrastructure, hybrid operations remain a latent risk. Coupled with the vastness of the maritime Indo-Pacific, the dual-use nature of commercial and state vessels makes attribution extremely challenging.[33] This increases the risk to underwater infrastructure by providing cover for deliberate sabotage or espionage, and complicating monitoring, attribution, and protective responses.
3. **Advancements in technology**: The convergence of cutting-edge technologies such as robotics, sensors, AI, and autonomous systems and/or surface vessels has significantly enhanced the ability to damage or disrupt CUI. These technologies, once the domain of powerful state actors, are now increasingly accessible to smaller states, criminal groups, and terrorist organisations.[34]
4. **Regulatory fragmentation and constraints:** Many Southeast Asian states maintain differing interpretations of UNCLOS provisions. Few ASEAN states explicitly criminalise intentional damage to submarine cables or have implemented Article 113 of UNCLOS in domestic law – none have implemented express legislation on "protection of subsea cables and pipelines".[35] Some states impose cabotage requirements or licensing schemes

---

30 Aylin Matlé, "Security Risks in the Indo-Pacific", *German Council on Foreign Relations (DGAP)*, September 18, 2024, https://dgap.org/en/research/publications/security-risks-indo-pacific

31 Shreya Gautam, Ronald Rapp, Richard Kram, Jonathan Liss, and Richard Pierce, "PHYSICAL and CYBER SECURITY for UNDERSEA CABLES in an OPEN CABLE ENVIRONMENT," *SubOptic (*April 2019). https://www.researchgate.net/publication/384676817_PHYSICAL_AND_CYBER_SECURITY_FOR_UNDERSEA_CABLES_IN_AN_OPEN_CABLE_ENVIRONMENT.

32 For instance, while Singapore has suggested an intention to declare an EEZ, it has yet to delineate its boundaries with its immediate neighbours. See: Salma Yusof, Mazura Md Saman, and Khairul Nizam Taib, "Malaysia-Singapore Maritime Delimitation: A Complex Path of Resolution?", *International Journal of Law, Government and Communication*, 9(37), September 2024, pp. 154-164 (p. 160), https://gaexcellence.com/ijlgc/article/view/4194

33 For example, Russia's use of commercial vessels such as *Eagle S* for hybrid warfare. See: Seth G. Jones, "Russia's Shadow War Against the West", *CSIS*, March 18, 2025, https://www.csis.org/analysis/russias-shadow-war-against-west

34 van Soest, *Protecting Europe's Critical Undersea Infrastructure Depends on Coordination and Collaboration*.

35 Wai Mon Su, "Protection of Submarine Cables and Pipelines: The Legal and Regulatory Practices of ASEAN Member States", Centre of International Law, National University of Singapore, 2025, https://cil.nus.edu.sg/wp-content/uploads/2025/09/Session-2-Dr.-SU-Wai-Mon-Protection-of-Submarine-Cables-and-Pipelines-The-Legal-and-Regulatory-Practices-of-ASEAN-Member-States.pdf

for foreign repair ships, often delaying emergency maintenance (see section 1.2). These disparities slow regional coordination and weaken deterrence.

5. **Economic dependencies and limited redundancy:** As most ASEAN states are developing economies with relatively limited naval assets, they may rely on commercial repair contractors (e.g., from Singapore). A typical repair permit can take 40 days to process, leaving cables vulnerable to prolonged outages.[36]

1.1.4.3. Implications for Singapore

Singapore's role as a global connectivity hub makes it highly dependent on secure and resilient subsea systems, which means it must balance commercial openness with infrastructure security. Any major disruption could have disproportionate consequences (e.g., relating to global data flows and financial systems). The priority therefore lies in building layered resilience through both technical and institutional means.

Another key policy tension lies between Singapore's high level of technical capacity and the limited jurisdictional reach of its maritime zone. As the smallest coastal state among its immediate neighbours, Singapore depends on close coordination with partners to ensure regional situational awareness and rapid incident responses. Strengthening cross-border cooperation, surveillance, and private-sector partnerships is essential to safeguard regional CUI resilience amid growing hybrid and geopolitical risks.

Considering the above dynamic, initiatives to protect subsea infrastructure should remain proportionate and consistent with the region's preference for non-escalatory approaches. Over-securitisation could risk alienating neighbours or fuelling regional mistrust, while under-securitisation could expose Singapore to potentially catastrophic data and trade disruptions.

1.1.5. Current initiatives to counter CUI threats in Singapore

1.1.5.1. National initiatives

Singapore's protection of subsea infrastructure at the national level is guided by a combination of legislative and regulatory frameworks. The Infocomm Media Development Authority (IMDA) is the main governmental body regarding subsea cables, oversees cable operations, repair permits, and incident reporting protocols.[37] The ones require operators to "promptly" notify the government following any cable cut or disruption.[38] The Telecommunications Act (2022) criminalises intentional damage to submarine cables within Singapore's territorial waters.[39]

---

36 Submarine Telecoms Industry Report, issue 12, Submarine Telecoms Forum, October 26, 2023, p. 84, https://issuu.com/subtelforum/docs/submarine_telecoms_industry_report_issue_12.

37 GUIDELINES ON THE MANAGEMENT OF SUBMARINE CABLE DAMAGE INCIDENTS IN SINGAPORE PORT LIMITS AND THE TRAFFIC SEPARATION SCHEME ZONE (2020), https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/codes-of-practice-and-guidelines/guidelines-on-the-management-of-submarine-cable-incidents-revised6oct2020.pdf.

38 Erin L. Murphy and Bryja, *The Strategic Future of Subsea Cables*.

39 Erin Murphy and Thomas Bryja, *The Strategic Future of Subsea Cables* (Center for Strategic & International Studies, 2025), 4.

Complimenting these efforts, the Cybersecurity Act (2018) establishes a legal framework to oversee the protection of Critical Information Infrastructure (CII) and information systems.[40] The succeeding 2021 Singapore Cybersecurity Strategy built on these foundations outlining three "strategic pillars": Building resilient infrastructure, enabling a safer cyberspace, and improving international cyber cooperation.[41] Taken together, these measures extend protection beyond physical assets to include the digital control systems that manage them.

Singapore has also introduced procedural streamlining for repair approvals and expanded public-private coordination with cable operators.[42] Additionally, the Maritime and Port Authority (MPA) works closely with IMDA and the Cyber Security Agency (CSA) to regulate maritime and information-security aspects of subsea operations. Notably, MPA and IMDA have partnered to explore 5G use cases in maritime operations.[43] The organizations have also co-developed a Maritime Digitalisation Playbook to help companies develop digital transition strategies.[44] MPA also previously collaborated with CSA to launch a Maritime Security Operations Centre in 2019 (now the Maritime Cyber Assurance and Operations Centre).[45] In theory, this coordination between agencies would also help to mitigate the risk of overlapping jurisdictions between maritime and digital regulators.

1.1.5.2. **International initiatives**

Singapore's international approach is centred on multilateral cooperation under ASEAN and related frameworks, including active involvement in regional multilateral efforts to secure maritime routes and communication cables. Since 2013, ASEAN ministers have held regular Telecommunications and Information Technology Ministers' Meetings (now titled ASEAN Digital Ministers' Meetings (ADGMIN)), in a recognition of the critical importance of subsea cable networks and agreed on increased cooperation to protect these networks from threats.[46] The 2019 ASEAN guidelines on Strengthening Resilience and Repair of Submarine Cables further simplified regional permitting and maintenance procedures.[47] In February 2024 and January 2025, ADGMIN "reiterated these commitments, announcing plans to "build a secure, diverse and resilient submarine cable network" and facilitate regional cooperation in deploying, repairing, and protecting cables."[48]

---

40 "Cybersecurity Act 2018 - Singapore Statutes Online", Part 3, Sso.agc.gov.sg, 2018, https://sso.agc.gov.sg/Acts-Supp/9-2018/.

41 "The Singapore Cybersecurity Strategy 2021", Cyber Security Agency of Singapore, 2021, https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021/.

42 Soham Agarwal, "Enhancing Capacity-of and Capabilities-in Repair of Submarine Communication Cables through International Cooperation", *National Maritime Foundation*, 2024, p. 4 & 6, https://maritimeindia.org/wp-content/uploads/2024/05/Soham-Agarwal-Cable-Repair-through-International-Cooperation-.pdf

43 "5G Innovation," Infocomm Media Development Authority, n.d. https://www.imda.gov.sg/how-we-can-help/5g-innovation.

44 Rob O'Dwyer, "Singapore Launches Maritime Digitalisation Playbook to Accelerate Economic Reboot - Smart Maritime Network," *Smart Maritime Network*, June 23, 2020, https://smartmaritimenetwork.com/2020/06/23/singapore-launches-maritime-digitalisation-playbook-to-accelerate-economic-reboot/.

45 "New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness", Maritime & Port Authority of Singapore (MPA), 16 May 2019, https://www.mpa.gov.sg/media-centre/details/new-24-7-maritime-cybersecurity-operations-centre-to-boost-cyber-defence-readiness.

46 Erin L. Murphy and Bryja, *The Strategic Future of Subsea Cables*.

47 "ASEAN TELECOMMUNICATIONS and INFORMATION TECHNOLOGY MINISTERS MEETING (TELMIN) ASEAN GUIDELINES for STRENGTHENING RESILIENCE and REPAIR of SUBMARINE CABLES." n.d. https://asean.org/wp-content/uploads/2012/05/ASEAN-Guidelines-for-Strengthening-Resilience-and-Repair-of-Submarine-Ca....pdf.

48 Erin Murphy and Bryja, *The Strategic Future of Subsea Cables*, 5.

Singapore currently chairs the ASEAN Working Group on Submarine Cables, which promotes information sharing and capacity building among member states.[49] These efforts complement broader regional security initiatives, including the Information Fusion Centre (IFC),[50] and the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP),[51] which are both platforms that could potentially be adapted to include the monitoring of cable-related incidents. However, most ASEAN instruments remain "soft law" and depend on voluntary compliance rather than binding obligations.[52]

Beyond ASEAN, Singapore has signed a Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World alongside the EU, promoting the use of secure and verifiable vendors in cable construction and maintenance.[53] This alignment reflects Singapore's growing role in shaping global norms around digital and infrastructure security, though it must still navigate sensitivities regarding the bifurcation of global supply chains between "trusted" and "untrusted" vendors.

1.1.6. Conclusion

CUI in both Europe and Asia faces a complex and evolving risk environment, driven by a combination of geopolitical tensions, technological advances, and economic dependencies. The Netherlands and Singapore, despite differences in scale and regional context, share similar vulnerabilities, including exposure to grey zone activities, state-led military actions, and accidental damage. These threats are amplified by the increasing accessibility of disruptive technologies and the concentration of maritime traffic in strategic corridors.

The Netherlands' approach to securing CUI reflects a mature and multilayered model combining technological capabilities with institutional coordination. Significant progress has been achieved through national initiatives and the establishment of cooperative platforms e.g., NorthSeal and SeaSEC. These measures collectively strengthen detection and resilience.

The threat landscape facing Singapore's subsea infrastructure is shaped most significantly by overlapping maritime jurisdictions and regulatory diversity. While intentional attacks remain rare, a combination of heavy maritime activity, limited redundancy, and prolonged repair times constitutes a significant strategic risk. Singapore's approach is similarly based on technical resilience and regional cooperation, helping to position it as a pragmatic leader in Southeast Asia's complex maritime environment.

---

49 Mario Masaya, Andrew Koch, Jileen Yong, Maya Crowden, Eleanor Ding, "Southeast Asia Calls For Cable Protection As Development Surges", *US-ASEAN Business Council*, 27 October, 2025, https://www.usasean.org/article/southeast-asia-calls-subsea-cable-protection-development-surges

50 "About IFC", Information Fusion Centre, n.d., https://www.ifc.org.sg/ifc2web/app_pages/User/commonv2/aboutus.cshtml.

51 "About ReCAAP Information Sharing Centre", *ReCAAP Information Sharing Centre*, n.d., https://www.recaap.org/about_ReCAAP-ISC

52 Didi Jubaidi and Dyah Ersita Yustanti,. "Soft Law Strategy in the ASEAN Charter Framework." *China Quarterly of International Strategic Studies* 11(1), June 2025, pp. 39–57, https://doi.org/10.1142/s2377740025500034.

53 "Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World," Ministry of Foreign Affairs, Singapore, 27 September, 2024, https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2024/09/Joint-Statement-on-the-Security-and-Resilience-of-Undersea-Cables-in-a-Globally-Digitalized-World

1.2. Challenges and policy gaps

Having examined the threat landscapes in Asia and Europe and the current governmental responses of Singapore and the Netherlands, this section turns to the policy gaps and challenges that continue to hinder the protection of CUI. Despite growing awareness of the threat environment, both regions face persistent limitations in their legal frameworks, resource allocation, and coordination mechanisms. Identifying these gaps is crucial for developing a coherent and credible deterrence posture.

1.2.1. Legal and normative limitations

The existing international legal regime governing underwater infrastructure is fragmented, outdated, and ill-suited to contemporary hybrid threat environments. Five core challenges stand out:

1. **Limited scope and participation.**
   The conventions addressing undersea cables, beginning with the 1884 Paris Convention, apply to a narrow set of activities and have limited ratification. It is unsurprisingly poorly equipped to address modern, non-traditional hybrid and grey-zone activities below the threshold of armed conflict. Many coastal and maritime powers are not party to them, leaving significant gaps in global coverage. Regional differences compound the problem – where European mechanisms rely significantly on codified EU and NATO frameworks, whereas ASEAN's non-supranational nature limits enforcement in Southeast Asia to voluntary compliance. As a result, intentional damage to cables in the high seas or in exclusive economic zones (EEZs) may fall into legal grey areas where enforcement is uncertain.[54]

2. **Weak enforcement and attribution mechanisms.**
   Even with improved surveillance technologies, attribution remains arguably the weakest link in deterrence. The difficulty of distinguishing between accident and intent (especially in congested maritime areas with heavy traffic) renders most incidents inconclusive. Current frameworks lack clear procedures for inspection, interdiction, or prosecution of suspected saboteurs. For instance, while the 1884 Convention recognized a right to board and inspect vessels suspected of damaging cables, this provision was not carried forward into later treaties such as UNCLOS. Without such mechanisms, states have few lawful means to verify or respond to hostile activity without risking escalation.[55] Moreover, smaller states may find it more practical to prioritise "mundane" resilience measures (e.g., redundancy and maintenance capacity) over costly attempts at perfect attribution.

3. **Insufficient alignment with hybrid and peacetime threats.**
   Most existing treaties were designed for a pre-digital, pre-hybrid era. They do not adequately address non-kinetic interference, cyber-enabled operations, or deliberate disruptions conducted below the threshold of armed conflict. As a result, hostile actions can often be framed as accidents or unprovable incidents, exploiting the normative gap between peacetime law and wartime conduct.[56]

---

54 Alexander Lott, *Unconventional Legal Approaches to Protecting Underwater Infrastructure* (The Hague Centre for Strategic Studies (HCSS), 2025), https://hcss.nl/report/unconventional-legal-approaches-protecting-underwater-infrastructure/.

55 'Battle of the Baltic: Safeguarding Critical Undersea Infrastructure', accessed 22 October 2025, https://www.epc.eu/publication/Battle-of-the-Baltic-Safeguarding-critical-undersea-infrastructure-645780/; Alexander Lott, *Unconventional Legal Approaches to Protecting Underwater Infrastructure*.

56 'Battle of the Baltic'.

4. **Absence of liability and compensation mechanisms.**
   The lack of clear provisions for civil liability means that states or private operators have limited recourse for claiming damages.[57] This discourages investment in preventive measures and weakens incentives for international cooperation on shared security standards. Moreover, an absence of timely prosecution procedures can allow incidents to linger without resolution.

5. **Lack of coordination over legislation, policy, and information sharing.**
   Fragmentation across national and regional boundaries can hinder cohesive action. In particular, Southeast Asia's patchwork of national laws and regulations creates added complexity. Some Southeast Asian states impose cabotage requirements or licensing schemes for foreign repair ships, often delaying emergency maintenance. Most notably, Indonesia maintains multiple overlapping ministerial decrees governing cable operations,[58] including cabotage laws.[59] Furthermore, while useful, public–private partnerships may be ad hoc, with unclear delineation of responsibilities. Although information sharing is more institutionalised in Europe (e.g., supported by continuous, all-hours operational centres),[60] efforts in Southeast Asia largely depend on voluntary exchanges through ASEAN.

Together, these limitations make the current legal order ill-equipped to deter or respond to deliberate sabotage of underwater infrastructure. They also generate ambiguity around acceptable defensive behaviour, increasing the risk of miscalculation at sea.

1.2.2. Monitoring and attribution challenges

Effective monitoring of CUI remains a major technological and operational gap. Even where surveillance systems exist, they are limited by coverage, data integration, and attribution capability. The difficulties in attribution make the implementation of effective responsive more difficult.

1. **Technical limitations**
   Most monitoring relies on sparse sensors, periodic inspections, or commercially owned systems that were not designed for security purposes. The vastness of oceanic networks makes real-time observation impossible. Autonomous underwater vehicles (AUVs) and seabed sensors are improving detection, but their deployment remains limited and costly.[61]

---

57 'Battle of the Baltic'.

58 Trissia Wijaya, "Regulatory Risks Key Barrier to Investment in Submarine Cables," *The Jakarta Post*, February 23, 2023. https://www.thejakartapost.com/paper/2023/02/24/regulatory-risks-key-barrier-to-investment-in-submarine-cables.html.

59 "Ownership, Cabotage and Flag Issues Relating to Indonesian Maritime Assets (Part I)", *Watson Farley & Williams*, September 2016, https://www.wfw.com/wp-content/uploads/2019/07/WFW-Indonesia-1.pdf; "Update on Indonesian Cabotage Rules", *Mochtar Karuwin Komar*, September 2024, https://www.mkklaw.net/static/mediamkk/newsletters/Update_on_Indonesian_Cabotage_Rules.pdf. See also: "New Rules Introduce Further Barriers to Foreign Direct Investment in Domestic Shipping Sector," *ABNR*, 30 December, 2024, https://www.abnrlaw.com/news/new-rules-introduce-further-barriers-to-foreign-direct-investment-in-domestic-shipping-sector.

60 A relevant example is the Common information sharing environment comprised of "EU maritime authorities, both civil and military, across borders and sectors". See: "Common information sharing environment (CISE)", *European Commission*, n. d., https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en

61 Giacomo Leccese and Ivan Zaccagnini, 'Securing the Depths: Rethinking EU Critical Infrastructure Protection in a Contested Underwater Domain', *CSDS*, 6 May 2025, https://csds.vub.be/publication/securing-the-depths-rethinking-eu-critical-infrastructure-protection-in-a-contested-underwater-domain/; *NATO Report on Protecting Critical Maritime Infrastructure* (European Commission, 2023), https://ec.europa.eu/newsroom/cipr/items/806192/.

2. **Attribution uncertainty**
   Even when a disruption is detected, distinguishing between accidental damage, natural causes, and deliberate interference is difficult. The subsea environment offers anonymity; actors can operate covertly with little traceability, enabling plausible deniability.[62]

3. **Hybrid and cyber convergence**
   As cable management systems and energy interconnectors increasingly rely on digital control networks, they become susceptible to cyber manipulation. Hybrid attacks can therefore blur the line between physical sabotage and data interference, complicating both detection and legal attribution.[63]

The absence of robust, shared monitoring architectures and attribution standards significantly limits deterrence, crisis management, and coordinated response. Without credible evidence, even serious incidents may go unpunished or unresolved.

1.2.3. Defensibility and costs

Protecting CUI is both technically difficult and economically burdensome. Most CUI lacking specialized defence systems or protective measures. Its primary safeguard is its isolation, but this same remoteness limits its defensibility, making rapid response or physical protection extremely challenging. The vast scale and global distribution of CUI networks further complicate efforts to maintain surveillance or deploy defensive assets, rendering comprehensive protection both logistically and financially complicated.[64]

Additionally, attackers can cause significant disruption with minimal resources, while defenders face immense costs, creating defensive asymmetry. Repairing a single damaged cable can cost between USD 1-3 million, and even brief outages can generate cascading economic effects.

Approximate disruption costs include:

- Telecommunications cables: €24 million per day, with repairs taking up to three weeks (≈ €504 million total).
- Electricity interconnectors: €12 million per day, repairs up to 60 days (≈ €720 million total).
- Oil and gas pipelines: €36 million and €75 million per day respectively, with repair times up to nine months, with total losses in the tens of billions of euros.[65]

This economic imbalance strongly favours offensive action and deters sustained investment in defensive readiness.[66]

---

62 Henri van Soest et al., *Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience* (RAND Europe, 2025), 13, https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3800/PEA3800-1/RAND_PEA3800-1.pdf?utm_.

63 van Soest et al., *Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience*.

64 *NATO Report on Protecting Critical Maritime Infrastructure*; van Soest, *Protecting Europe's Critical Undersea Infrastructure Depends on Coordination and Collaboration*.

65 van Soest et al., *Evolving Threats to Critical Undersea Infrastructure*.

66 Daniel Runde et al., *Safeguarding Subsea Cables* (Center for Strategic & International Studies, 2024), 7.

1.2.4. Policy coordination problems

Finally, the protection of CUI is undermined by institutional fragmentation and limited coordination across national and international levels.

1. **Public-private collaboration:**
   Since much of the infrastructure is privately owned, effective protection requires close coordination between government agencies and private operators, which can be challenging due to differing priorities. Additionally, responsibilities are often split between civilian regulators, military and maritime authorities, energy agencies, and private operators. This diffusion of authority delays decision-making and weakens accountability.[67]

2. **Cross-sector integration**:
   CUI spans multiple industries (e.g., energy, telecommunications, shipping), each governed by separate policies and agencies, creating difficulties in establishing unified protection strategies. Lack of information sharing practices can add to the difficulties.[68]

3. **International misalignment:**
   Cooperation between allies and regional partners remains largely ad hoc. The absence of shared situational awareness, standardized reporting, and interoperable crisis protocols reduces the effectiveness of collective deterrence. Additionally, often CUI crosses national boundaries or exist in areas with complex legal frameworks, requiring harmonization of laws and diplomatic cooperation between states.[69]

Strong CUI protection is hence hindered by the need to coordinate effectively between public and private actors, integrate policies across multiple industrial sectors, and harmonize legal and operational frameworks across international jurisdictions.

1.2.5. Conclusion

Despite substantial investments and initiatives in both the Netherlands and Singapore, the protection of CUI remains a complex and evolving challenge. Both countries face similar gaps and challenges, including legal ambiguities, monitoring limitations, high defence costs, and fragmented coordination.

Notwithstanding its achievements, the Dutch model still faces constraints that mirror those of other highly networked small states (e.g., a high concentration of privately owned maritime assets; limited naval coverage across a busy maritime space; a high cost of maintaining continuous surveillance and repair capabilities). The Netherlands continues to depend on both industry partnerships and multinational arrangements under the EU and NATO to fill these capability gaps. Here, adopting a strategy of complete control with regard to CUI protection is less feasible, while a strategy of adaptive governance is more ideal.

---

67 Christian Bueger and Tobias Liebetrau, 'Critical Maritime Infrastructure Protection: What's the Trouble?', *Marine Policy* 155 (September 2023): 105772, https://doi.org/10.1016/j.marpol.2023.105772; van Soest, *Protecting Europe's Critical Undersea Infrastructure Depends on Coordination and Collaboration*.

68 Christian Bueger et al., *Securing the Seas: A Comprehensive Assessment of Global Maritime Security* (United Nations Institute for Disarmament Research, 2024), https://unidir.org/publication/securing-the-seas-a-comprehensive-assessment-of-global-maritime-security/.

69 Bueger et al., *Securing the Seas*; Alexander Lott, *Unconventional Legal Approaches to Protecting Underwater Infrastructure*.

Singapore's maritime and digital centrality has positioned it at the heart of Southeast Asia's connectivity network (and correspondingly, its vulnerability). Most significantly, Singapore's small size and limited jurisdictional reach constrain unilateral action. Its challenge therefore lies in leading through facilitation (e.g., deepening regional coordination and public–private engagement), while avoiding over-securitisation that could unsettle the region's delicate maritime balance.

Altogether, addressing these issues requires not only continued technological innovation and strategic investment, but also strengthened public-private cooperation, enhanced international alignment, and robust interregional coordination.

Part 2.
A look at the future: enhancing prevention and enforcement at sea

2.1. Enhancing prevention and enforcement

As threats to CUI evolve, prevention and enforcement strategies must balance technological capability with legal clarity and cost realism. While outright sabotage remains rare, a combination of ageing legal instruments, fragmented governance, and uneven regional capabilities threatens to expose both Europe and Asia to vulnerability.

A future outlook is hence necessary to enhance prevention and enforcement at sea. The focus at large should be on three main areas:

- Hybrid threat preparedness: Integrate legal, technical, and geopolitical analysis to identify and counter grey zone tactics, military activities, and accidental damage.
- Attribution and deterrence frameworks: Establish clear policies for identifying actors, signalling accountability, and imposing consequences for deliberate interference.
- Regulatory innovation: Update national and international regulations to mandate protection, monitoring, and resilience measures for critical subsea infrastructure.

To achieve these broad goals, a series of measures can be taken:

2.1.1. Addressing legal and normative gaps

To overcome the fragmented and outdated international legal framework that limits deterrence and enforcement:

- **Clarify lawful defensive actions and thresholds for response:** Develop clear, internationally recognized rules of engagement for CUI protection that define when defensive measures, inspections, or interdictions are permissible, reducing the risk of miscalculation in peacetime or hybrid scenarios.
- **Strengthen civil liability and compensation frameworks:** Establish mechanisms for compensating operators for damages from accidents or deliberate attacks, incentivizing preventive investments and fostering cross-border cooperation on protection standards.
- **Update treaties to encompass hybrid threats:** Expand international agreements to explicitly address non-kinetic, cyber, and hybrid interference, ensuring that peacetime law keeps pace with modern threats.

- **The diffusion of norms:** Rather than pursuing entirely new legal treaties (which may encounter political resistance), an alternative strategy would be to proliferate existing (and consistent) understandings of responsible behaviour across cyber, maritime, telecommunications, and energy sectors.

2.1.2. Improving monitoring, detection, and attribution

To address the technological and operational limitations that hinder situational awareness and response:

- **Deploy distributed and integrated surveillance networks:** Combine seabed sensors, autonomous underwater vehicles (AUVs), satellite monitoring, and AI-driven anomaly detection to achieve near real-time observation across critical CUI nodes.
- **Develop standardized attribution protocols**: Establish internationally recognized methods to distinguish between accidents, natural events, and deliberate interference, enabling legal and diplomatic responses with confidence.
- **Integrate cyber and physical monitoring:** Ensure that digital control systems for cables, pipelines, and interconnectors are continuously monitored for cyber intrusions, linking cyber and physical incident data to detect hybrid threats early.

2.1.3. Reducing defensibility gaps and cost asymmetries

To mitigate the high economic and logistical burdens of CUI protection:

- **Implement redundancy and rapid repair frameworks:** Design alternative routes, backup interconnectors, and modular infrastructure to reduce single points of failure and limit the impact of attacks or accidents.
- **Prioritize protection for high-value or high-risk nodes:** Use risk-based strategies to allocate resources efficiently, focusing on chokepoints or areas with concentrated maritime traffic where disruption would be most severe.
- **Invest in preventive technologies**: Promote automation, remote monitoring, and smart protective barriers to reduce the need for constant human presence while lowering repair and operational costs.
- **Prioritise incremental redundancy:** Prior to investing in preventive technologies, more progressive steps (e.g., establishing additional landing points), can help to provide resilience without prohibitive expense.
- **Create a predictable environment for private investment and/or innovation:** Industry investment is more likely when governments signal consistent norms and commitments.

2.1.4. Strengthening public-private and international coordination

To overcome fragmented governance and limited cooperation:

- **Formalize public-private partnerships:** Establish dedicated coordination structures that clearly define responsibilities, share threat intelligence in real time, and align priorities between operators, regulators, and defence authorities. This may also include creating joint research and development grants between public universities and relevant industry players in both countries.
- **Enhance cross-sector integration:** Create unified protection frameworks that encompass energy, telecommunications, and shipping sectors. This would ensure consistent

standards, joint incident response protocols, as well as shared best practice exchanges and security dialogues (e.g., information sharing, repair coordination, and threat assessment).

- **Advance regional and international harmonization:** Develop interoperable crisis response exercises, standardized reporting, and coordinated deterrence policies among allies and partners to close gaps in international law enforcement and situational awareness.

2.1.5. Conclusion

In sum, safeguarding CUI requires a forward-looking approach that combines legal clarity, technological innovation, and coordinated governance. By addressing legal gaps, enhancing monitoring and attribution capabilities, mitigating defensibility challenges, and fostering robust public-private and international collaboration, states and operators can better anticipate, deter, and respond to evolving hybrid threats. Strengthening these interconnected measures will be essential to ensuring the resilience, security, and uninterrupted operation of vital subsea networks in an increasingly complex maritime environment.

2.2. Formulating of a comprehensive CUI protection agenda for Singapore and the Netherlands

Given the transnational and interconnected nature of CUI, effective prevention and enforcement cannot be confined to national or neighbouring-state frameworks alone. Threats to CUI cross maritime boundaries and require a coordinated approach that spans regions and legal jurisdictions. To effectively enhance prevention and enforcement at sea, cooperation must go beyond regional frameworks.

Strengthening international cooperation through interregional frameworks allows states to share intelligence, harmonize regulations, standardize attribution protocols, and conduct joint exercises, ensuring that deterrence and response measures are credible, timely, and proportionate. In this context, the Netherlands and Singapore are particularly well-positioned to lead collaborative initiatives: both are highly connected maritime hubs with advanced technological capabilities, robust public-private partnerships, and strategic roles in critical subsea networks. By leveraging their expertise and global linkages, they can serve as catalysts for broader interregional cooperation, setting standards and best practices that enhance the security, resilience, and sustainability of CUI worldwide. So what should be the main focus points for cooperation between Singapore and the Netherlands?

Despite their different security environments, the Netherlands and Singapore as international hubs of maritime activity face similar challenges. The rapid emergence of CUI into crucial elements of a nations' economic activity and data traffic has prevented the adaptation of existing legal frameworks and their evolution into suitable regulations for the protection of CUI. The complex jurisdiction and states' concern over their own strategic interests generally discourages the development of new laws and regulations.

The Netherlands and Singapore however have the possibility to encourage on the global stage the development of common norms and standards on the CUI through regional forums and groupings, highlighting states' mutual interests in collaborated action for their protection. These ones can help states reduce accident by shaping responsible behaviours of vessels and enhance monitoring and response measures. While they are not applicable to deliberately orchestrated incidents, the majority of cable cuts remains accidental. This mutual dependency however carries its own risks and requires states to maintain a large degree of transparency regarding their operations, control and jurisdiction over CUI, in relation to other states and to private actors. The governments' role and the ones of private actors must also be distinctive and transparent. The establishment of clear responsibilities and obligations between private and public actors is necessary for an efficient development of CUI protection.

Information sharing is a key element of the Dutch strategy, as a practice which enhances partners collaboration and response efficiency. With information sharing being a sensitive (especially in Southeast Asia) but highly efficient initiative, cooperation between the Netherlands and Singapore can be enhanced by the establishment of best practices, moving beyond incident reporting and focusing on proactive initiatives against damages.

The continuous technological advancements in CUI protection highlight investments in Research and Development as important windows for cooperation between states. While sensors, AI, and autonomous systems pose a rising threat to CUI, they can also be developed to increase resilience, monitoring and response to incidents. Encouraging cooperation between institutions such as Nanyang Technological University and TU Delft through grants offers the Netherlands and Singapore an opportunity, first to develop proactive and reactive systems based on common norms, but also to encourage public-private collaborated R&D, establishing the two countries as leaders in CUI development. The two countries already cooperate and exchange largely in water management and coastal resilience projects. Establishing CUI protection as another pillar of cooperation which mirrors the two other ones is an important step for the two countries to improve their cooperation.

Finally, the changing security environments and, more specifically, the intensification of great power competition in the Indo pacific between the US and China will require the Netherlands and Singapore transparency regarding their position with both countries. The creation of a security dialogue can ensure that the two countries' security assessment and policy decisions align. With China's claim over the South China Sea and complex issue of permits, anticipating potential conflicts will make the cooperation between the Netherlands and Singapore more efficient.

Conclusion

As the vulnerability of CUI increases, so do the incentives for Singapore and the Netherlands to increase bilateral cooperation on the matter. Both states face various challenges in the protection of CUI. Rapidly changing technologies have made current legal frameworks outdated and unsuitable for the establishment of an international governance of CUI. The hybrid environment also contributes to exacerbate the gap between current regulations and necessary ones to efficiently protect CUI. Effective monitoring and attribution of CUI related incidents are also major issues posed due to limited technological capabilities, but also due to the burdening cost of maintenance and reparations. Finally, the limited agreements and coordination between national policies prevent international, effective protection.

Investments in the development of protective measures at national and international levels to enhance prevention, monitoring, and response strategies against CUI related incidents are underway in both Singapore and the Netherlands. Still, considerable policy gaps and challenges remain. Some of these can be addressed by enhancing bilateral cooperation.

Implementing intelligence and monitoring processes as an integral part of the protection allows the Netherlands and Singapore to move beyond reactive measures to cable cuts towards proactive initiative, higher accountability and a better conceptualization of risks posed. The establishment of commonly agreed norms regarding the protection of CUI is also becoming necessary, first to redefine and readjust jurisdiction over CUI in international water, but also to encourage accountability and cooperation in highly critical regions. Coordinated R&D also enhances cooperation while contributing to fill the technological gap preventing efficient monitoring and surveillance. This collaboration will also require the two states to address US-China competition in the Indo-Pacific region to ensure coordinated threat assessment and effective policy decisions on protection of CUI.

A comprehensive agenda for cooperation on CUI between the Netherlands and Singapore must aim at (a) enhancing CUI resilience; (b) strengthening bilateral ties; (c) setting the standards for international cooperation on CUI. By implementing the abovementioned measures, Singapore and the Netherlands can increase the protection of assets critical to national security and societal resilience while simultaneously opening new venues of bilateral cooperation. Furthermore, the highly international nature of CUI makes it the perfect area for enhancing cooperation between European and Indo-Pacific states. Singapore and the Netherlands have the chance to lead these efforts and set the standards for maritime security cooperation between small and middle powers that have much to gain from standing together in the face of increased great power competition.

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl