Hybrid CoE Research Report 14

Protecting maritime infrastructure from hybrid threats: legal options

Hybrid CoE

Aurel Sari – March 2025

Hybrid CoE Research Reports are thorough, in-depth studies providing a deep understanding of hybrid threats and phenomena relating to them. Research Reports build on an original idea and follow academic research report standards, presenting new research findings. They provide either policy-relevant recommendations or practical conclusions.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 | www.hybridcoe.fi

ISBN 978–952–7591–20–8 (web)
ISBN 978–952–7591–21–5 (print)
ISSN 2737–0860 (web)
ISSN 2814–7219 (print)

March 2025

Cover photo: Bradley Pietzyk / shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

Summary

This report examines the legal authorities available to states under the law of the sea to counter hybrid threats against critical maritime infrastructure. Building on an expert workshop hosted by Hybrid CoE in November 2024, it takes stock of and informs ongoing work in this area in the context of Russia's armed aggression against Ukraine and recent incidents in the Baltic and North Seas.

Maritime infrastructure supports a range of essential services. The critical contribution made by maritime assets across the EU and NATO has heightened concerns over their vulnerability to sabotage and other deliberate attacks, including those forming part of a hybrid campaign. The report distinguishes between five categories of assets and suggests that addressing maritime hybrid threats requires a multifaceted approach involving three complementary lines of effort: maintaining situational awareness, taking operational action, and increasing resilience.

Carrying out these tasks requires appropriate legal authorities. The law of the sea establishes jurisdictional zones that delineate the rights and responsibilities of coastal and other states. The report shows that these rules confer broad authorities on coastal states to maintain situational awareness of maritime hybrid threats. However, the legal framework is less robust when it comes to taking operational action. This is because the zonal logic of the law of the sea does not sit well with the character and vulnerabilities of certain categories of maritime infrastructure. The report suggests that significant gaps exist in the legal protection of submarine communication cables in particular, before discussing the impact of the rules governing the use of force.

The report recommends that EU and NATO member states should make sure to exercise their prescriptive jurisdiction under UNCLOS to its full extent; strengthen collaboration between different national authorities in exercising their enforcement powers; explore the extent to which dynamic or innovative interpretations of existing rules may address gaps in the regulatory framework; reinforce information sharing and collective attribution; and make diplomatic efforts to strengthen international cooperation for the protection of critical maritime infrastructure.

1. Introduction

The resources and benefits derived from the marine environment are critical to daily life.[1] With over 80% of goods transported by sea, the oceans are indispensable for international trade and commerce. They provide food and income for a large part of humanity, while marine industries such as shipping and tourism contribute trillions of dollars to the global economy. However, these benefits cannot be realized without an extensive network of maritime infrastructure. Vessels need navigational aids to find their way. Maritime transport and tourism rely on terminals for boarding. Offshore energy production requires rigs, platforms and pipelines.

Maritime infrastructure is vulnerable to a range of threats. Natural disasters, accidents and deliberate attacks on critical nodes can have far-reaching consequences across multiple industries, affecting everything from manufacturing to national security.[2] This makes maritime infrastructure a prime target for hybrid threats. Not only are many maritime assets vulnerable to attack, but disrupting the essential services they provide may cause significant economic, financial, and societal harm. The vast size of the marine environment gives malign actors ample opportunities to evade detection and attribution. At the same time, it presents real difficulties for nations seeking to protect their facilities from interference.

These dangers are not merely hypothetical. In 2017, the NotPetya malware attack severely disrupted the operations of Maersk, one of the world's largest shipping companies.[3] Concerns have been raised that the Arctic has become a renewed target of Russian hybrid threats.[4] In recent years, a spate of suspected hybrid attacks has occurred in the North Sea and the Baltic Sea, including the sabotage of the Nord Stream 2 pipeline in 2022,[5] the ongoing spoofing of the automatic identification system (AIS) used for navigation,[6] and the cutting of submarine communication cables in 2022 and 2024.[7]

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) has included maritime hybrid threats in its programme of

1 For a general overview, see Hance D. Smith, Juan Luis Suárez de Vivero and Tundi S. Agardy, 'The World Ocean and The Human Past and Present', in *Routledge Handbook of Ocean Resources and Management*, ed. Hance D. Smith, Juan Luis Suárez de Vivero and Tundi S. Agardy (London: Routledge, 2015), 5–13.

2 E.g. Nguyen Khoi Tran, et al., 'The Costs of Maritime Supply Chain Disruptions: The Case of the Suez Canal Blockage by the 'Ever Given' Megaship', *International Journal of Production Economics*, Volume 279 (2025): 1–16.

3 Warwick Ashford, 'NotPetya attack cost up to $300m, says Maersk', *Computer Weekly*, 17 August 2017, https://www.computerweekly.com/news/450424559/NotPetya-attack-cost-up-to-300m-says-Maersk.

4 Cecilie Juul Stensrud and Andreas Østhagen, 'Hybrid Warfare at Sea? Russia, Svalbard and the Arctic', *Scandinavian Journal of Military Studies*, Volume 7 (2024): 111–130; Andreas Østhagen, 'The Arctic after Russia's Invasion of Ukraine: The Increased Risk of Conflict and Hybrid Threats', Hybrid CoE Paper 18 (The European Centre of Excellence for Countering Hybrid Threats, 2023).

5 Matthias von Hein, 'Nord Stream Pipelines Blasts: A Maze of Speculation', Deutsche Welle, 25 September 2023, https://www.dw.com/en/nord-stream-pipelines-blasts-a-maze-of-speculation/a-66913853.

6 Elisabeth Braw, 'The Baltic Sea's Bad Actors', *Foreign Policy*, 4 December 2024, https://foreignpolicy.com/2024/12/04/russia-china-baltic-sea-nato-subsea-cables-ais-spoofing/.

7 Anne Kauranen and Nerijus Adomaitis, 'Recent Suspected Underwater Sabotage Incidents in the Baltic Sea', Reuters, 3 December 2024, https://www.reuters.com/world/europe/recent-suspected-underwater-sabotage-incidents-baltic-sea-2024-12-03/.

work since its establishment. One strand of this work has focused on legal questions.[8] International law, particularly the law of the sea, plays a critical role in this area. Hybrid threat actors exploit the applicable rules to pursue their strategic objectives, whether by taking advantage of regulatory gaps, circumventing their obligations, or falsely portraying their actions as legally justified. For EU member states and NATO allies, international law serves as a normative framework that provides them with legal authorities, processes and instruments to counter hybrid threats in the maritime domain.[9] A persistent concern in this respect is whether the applicable rules enable member states to safeguard their interests effectively.[10]

On 28 November 2024, Hybrid CoE convened a one-day workshop to explore these issues in the light of recent developments.[11] This report draws together and builds on these discussions with the aim of informing ongoing efforts to counter hybrid threats against critical maritime infrastructure. Section 2 of the report takes a closer look at maritime infrastructure to distinguish between different categories of assets, the threats they face, and how they may be protected. Section 3 offers an overview of the different jurisdictional zones established under the law of the sea and the authorities they confer on states to maintain situational awareness in the marine environment and to take operational action in response to hybrid threats. Section 4 provides an overall assessment of the legal authorities for countering maritime hybrid threats, before focusing on the challenges posed by submarine communication cables and the application of rules governing the use of force. Section 5 presents some concluding thoughts and recommendations.

8 In particular, see Georgios Giannoulis (ed), 'Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans', Hybrid CoE Paper 16 (The European Centre of Excellence for Countering Hybrid Threats, 2023).

9 See Council of the European Union, 'Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns', Council Doc. 10016/22, 21 June 2022, 5 (declaring that a coordinated EU response to a hybrid campaign should respect international law).

10 Generally, see David Letts, 'The Maritime Domain', in *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, ed. Mitt Regan and Aurel Sari (New York: Oxford University Press, 2024), 251–270; Alexander Lott (ed.) *Maritime Security Law in Hybrid Warfare* (Brill 2024); Alexander Lott, *Hybrid Threats and the Law of the Sea: Use of Force and Discriminatory Navigational Restrictions in Straits* (Leiden: Brill, 2022).

11 The workshop brought together senior experts to discuss the legal questions raised by threats to submarine infrastructure, the ongoing tensions in the South China Sea, and the strategic importance of the North-East Passage. External participants included Emeritus Professor Terry Gill (University of Amsterdam), Professor Wolff Heintschel von Heinegg (Europa-Universität Viadrina), Professor James Kraska (Stockton Center for International Law), Professor Aurel Sari (University of Exeter) and Junior Professor Dr Valentin Schatz (Leuphana University).

2. Critical maritime infrastructure

The need to safeguard maritime infrastructure against hostile interference is widely recognized. For example, the Revised EU Maritime Security Strategy (EUMSS) of 2023 declares the protection of 'critical infrastructure in the maritime domain' to be a top priority.[12] Notwithstanding such declarations, it has become clear against the backdrop of recent incidents and Russia's ongoing war in Ukraine that maritime assets remain vulnerable to sabotage and disruption.[13] One of the recommendations made in 2023 by the EU-NATO Task Force on the resilience of critical infrastructure was to explore options for 'how to improve the monitoring and protection of critical infrastructure in the maritime domain by relevant authorities'.[14]

Clearly, monitoring and protecting maritime infrastructure is a complex task. Maritime infrastructure consists of highly diverse categories of assets. For example, oil pipelines traversing the ocean floor differ fundamentally in their function and key features from lighthouses and fish processing plants. Not all threats target the same vulnerabilities. The cutting of submarine communication cables has different effects, impacting different sectors, than the obstruction of a maritime chokepoint. Distinct threats also call for different responses. Being well prepared for natural disasters may offer little help in the fight against maritime piracy.

The complexity of safeguarding maritime infrastructure has important legal implications, since diverse categories of assets, threats and response options raise distinct legal questions. This section provides a brief overview of these points.

2.1 Categories of maritime infrastructure

Critical infrastructure encompasses a wide range of assets, networks, and systems. This is reflected in general definitions of the term, such as the one adopted in the EU's 2022 Directive on the Resilience of Critical Entities. The Directive defines critical infrastructure as 'an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service'.[15] An essential service, in turn, is defined as 'a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment'.[16] These are rather broad definitions. Ultimately, whether something qualifies as critical infrastructure depends on how important a contribution it makes to core societal and environmental processes. However, this tells us very little about the nature of an asset and its features, significance, or vulnerabilities. Transposing the notion into the maritime domain leads to similarly broad and somewhat unhelpful definitions. Accordingly, critical maritime infrastructure has been described as the essential assets, facilities, systems, networks, and processes that support

12 'Revised EU Maritime Security Strategy', Annex I to the Annex to 'Council Conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan', Council doc. 14280/23, 24 October 2023, 5, 29.
13 European Commission, 'White Paper: How to Master Europe's Digital Infrastructure Needs?', COM(2024) 81 final, 21 February 2024, 18–19.
14 NATO-EU Task Force on the Resilience of Critical Infrastructure, 'Final Assessment Report', 29 June 2023, 9.
15 Article 2(4), Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC, OJ [2022] L333/164.
16 Article 2(5), Directive (EU) 2022/2557.

the security, safety, and stability of maritime operations.[17]

Clearly, it is necessary to distinguish between different types of maritime infrastructure at a more granular level. One established approach is to categorize assets based on their association with different sectors.[18]

The first category includes assets and facilities associated with shipping, including vessels of all types, shipping lanes, maritime chokepoints, ports and terminals, and navigational aids, such as lighthouses, buoys, beacons, and advanced electronic systems like the automatic identification system (AIS) and the global positioning system (GPS).

The second group consists of infrastructure required for energy production. This includes facilities and equipment for subsea extraction and transport of fossil fuels, such as oil and gas platforms, drilling rigs and pipelines, as well as installations for the generation of renewable energy, such as offshore wind farms, wave and tidal platforms and the submarine energy cables that service them.

The third includes communication infrastructure, particularly submarine communication cables and associated equipment, such as repeaters and landing points.

The fourth category covers fishing infrastructure, including equipment for harvesting, processing and distributing marine resources, such as fishing vessels, processing plants, aquaculture platforms, and fishery zones, as well as tools that facilitate fishing, such as navigation and monitoring systems.

The fifth category represents the marine ecosystem and the living species it contains. Traditionally, the concept of infrastructure has been associated with physical and built systems, rather than the natural environment. However, viewing the marine ecosystem as a form of natural infrastructure underlines its role in delivering vital services, such as climate regulation, coastal protection, and biodiversity, which in turn underpin other maritime activities, such as tourism and fishing.

2.2 Threats posed by deliberate harm

Maritime infrastructure faces threats from three directions. First, it is exposed to environmental risks, such as extreme weather events and climate change.[19] Second, it is vulnerable to accidental damage caused by human error, technical malfunction or a combination of both.[20] Third, maritime infrastructure is also at risk from deliberate harm, such as armed conflict, geopolitical confrontation, piracy, acts of terrorism, sabotage and hybrid threats.

Due to its strategic character, maritime infrastructure is often deliberately targeted during armed conflict. For example, as part of its aggression against Ukraine, Russia has carried out numerous attacks against Ukrainian ports

17 Diren Doğan and Deniz Çetikli, 'Maritime Criticial Infrastructure Protection (MCIP) in a Changing Security Environment' (NATO Maritime Security Centre of Excellence, 2023), 10.

18 Christian Bueger and Tobias Liebetrau, 'Critical Maritime Infrastructure Protection: What's the Trouble?', *Marine Policy*, Volume 155 (2023): 1–8, 2.

19 E.g. Yoshio Kajitani, Stephanie E. Chang and Hirokazu Tatano, 'Economic Impacts of the 2011 Tohoku-Oki Earthquake and Tsunami', *Earthquake Spectra*, Volume 29 (2013): 457–478.

20 E.g. Greg Miller, 'Billions in Damage Claims Pile Up in Response to Baltimore Bridge Disaster', Lloyd's List, 24 September 2024, https://www.lloydslist.com/LL1150755/Billions-in-damage-claims-pile-up-in-response-to-Baltimore-bridge-disaster.

and grain-carrying vessels to undercut Ukraine's agricultural exports.[21] Disputes over the control of strategic waterways and maritime features are another source of tension and disruption. Examples include the confrontation between the People's Republic of China and other coastal nations in the South China Sea, and naval skirmishes between Iran and other Gulf states.

Inter-state conflicts and disputes are not the only source of deliberate threats to maritime infrastructure. Non-state actors may target ports, offshore energy installations and shipping routes to cause economic disruption, propagate fear or engage in armed conflict. Attacks by the Houthis on international shipping in the Red Sea provide an example of the latter.[22] Elsewhere, piracy remains a persistent threat, particularly in regions such as the Gulf of Guinea, the Strait of Malacca and off the coast of Somalia. Terrorist organizations have also turned to maritime infrastructure as a target for attack. In 2004, the terrorist group Abu Sayyaf planted a bomb on the Philippine-registered *MV SuperFerry 14*, destroying the vessel and killing 116 people.[23]

The increasing digitalization of maritime operations has rendered them vulnerable to cyberattacks. From navigation systems to port operations, critical maritime infrastructure depends on interconnected digital systems that can be exploited by malicious actors, including criminal networks. For example, in 2022, a cyberattack disrupted the operations of three global oil companies in the Port of Antwerp, while the Port of Lisbon suffered a ransomware attack in a separate incident.[24]

These different categories of deliberate harm are not mutually exclusive. In particular, hybrid threats may form an integral part of geopolitical confrontation or manifest themselves through acts of terrorism or cyber operations.

2.3 Situational awareness, operational action and resilience

Given the diverse categories of maritime infrastructure and their multiple vulnerabilities, protecting maritime assets against hybrid threats requires a comprehensive and multi-faceted approach. Since many critical facilities fall under more than one jurisdiction and their disruption may have cascading effects across the EU and NATO, coordination and cooperation among member states and allies is essential.[25] This need was recognized at the Baltic Sea NATO Allies

21 Caitlin Welsh, Joseph Glauber and Emma Dodd, 'Russia's Renewed Attacks on Ukraine's Grain Infrastructure: Why Now? What Next?', Center for Strategic and International Studies, 25 November 2024, https://www.csis.org/analysis/russias-renewed-attacks-ukraines-grain-infrastructure-why-now-what-next.

22 Theo Notteboom, Hercules Haralambides and Kevin Cullinane, 'The Red Sea Crisis: Ramifications for Vessel Operations, Shipping Networks, and Maritime Supply Chains', *Maritime Economics and Logistics*, Volume 26 (2024): 1–20; Emilio Rodriguez-Diaz, J. I. Alcaide and R. Garcia-Llave, 'Challenges and Security Risks in the Red Sea: Impact of Houthi Attacks on Maritime Traffic', *Journal of Marine Science and Engineering*, Volume 12 (2024): 1–18.

23 Peter Lehr, *A Modern History of Maritime Terrorism: From the Fenian Ram to Explosive-Laden Drone Boats* (Cheltenham: Edward Elgar, 2023), 114–118.

24 Chalermpong Senarak, 'Port Cyberattacks from 2011 to 2023: A Literature Review and Discussion of Selected Cases', *Maritime Economics and Logistics*, Volume 26 (2024): 105–130.

25 Norway, Ministry of Energy, 'Six North Sea Countries Join Forces to Secure Critical Infrastructure', 5 April 2024, https://www.regjeringen.no/contentassets/03b6ba0be17e4ea0a57517a771ab5d8b/20240409_press-release_six-north-sea-countries-join-forces-to-secure-critical-infrastructure.pdf.

Summit held in Helsinki on 14 January 2025.[26] As reflected in the Joint Statement adopted at the Summit,[27] protecting critical maritime infrastructure from deliberate harm involves three complementary lines of effort: situational awareness, operational action, and resilience.

First, any strategy for safeguarding maritime infrastructure must be based on a detailed understanding of the operating environment.[28] Maintaining situational awareness requires ongoing monitoring, surveillance and information gathering to detect hybrid threats. However, the nature of the maritime domain and the infrastructure concerned pose real challenges. For example, while undersea communication cables can be monitored to identify technical faults, it is more difficult to detect physical attacks against them in real time, given the immense length of these cables, the large number of surface vessels that may operate in their vicinity, and the ability of some hostile actors to conceal their actions by employing advanced capabilities.[29] Since nearly two-thirds of damage to submarine cables is accidental in nature,[30] a robust understanding of the situation is required to distinguish mere accidents from deliberate attacks. Compelling evidence is also necessary to attribute malicious acts to state or non-state perpetrators before they can be held to account. While new technologies may contribute to such monitoring and surveillance efforts,[31] novel technologies may also be utilized by hostile actors for malign purposes.

Second, protecting maritime infrastructure from hybrid threats requires the ability to take operational action to investigate, deter, prevent, interrupt and counter harmful activities. Individual EU member states and NATO allies are actively expanding their capabilities in this area.[32] The United Kingdom, for example, has invested in new vessels dedicated to underwater surveillance in areas of sovereign interest as part of its Multi-Role Ocean Surveillance (MROS) programme.[33] Deploying the available capabilities in response to unfolding incidents demands appropriate decision-making

26 Office of the President of the Republic of Finland, 'Security in the Baltic Sea Region to be Strengthened by Military Presence and Technological Innovations', 14 January 2025, https://www.presidentti.fi/en/security-in-the-baltic-sea-region-to-be-strengthened-by-military-presence-and-technological-innovations/.

27 Joint Statement of the Baltic Sea NATO Allies Summit, 14 January 2025, https://www.presidentti.fi/joint-statement-of-the-baltic-sea-nato-allies-summit/.

28 In the context of submarine cables, see the emphasis placed on assessment and information exchange by the European Commission, 'Recommendation on Secure and Resilient Submarine Cable Infrastructures', C(2024) 1181 final, 26 February 2024.

29 See Sidharth Kaushal, 'Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure', Royal United Services Institute, 25 May 2023, https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

30 Jonathan E. Hillman, 'Securing the Subsea Network: A Primer for Policymakers' (Center for Strategic and International Studies 2021), 8.

31 See G. Soldi et al., 'Monitoring of Critical Undersea Infrastructures: The Nord Stream and Other Recent Case Studies', *IEEE Aerospace and Electronic Systems Magazine*, Volume 38 (2023): 4–24.

32 Njall Trausti Fridbertsson, 'Protecting Critical Maritime Infrastructure: The Role of Technology, General Report', NATO Parliamentary Assembly, 032 STC 23 E rev.2 fin, 7 October 2023, 9–10.

33 Royal Navy, 'UK Protection Enhanced as Underwater Surveillance Ship Enters Service', 10 October 2023, https://www.royalnavy.mod.uk/news/2023/october/10/20231010-uk-protection-enhanced-as-underwater-surveillance-ship-enters-service.

structures and processes, including command and control arrangements for the use of military assets. At the 2023 Vilnius Summit, NATO Heads of State and Government decided to establish a Maritime Centre for the Security of Critical Undersea Infrastructure within NATO's Maritime Command (MARCOM).[34] Established in 2024, the Centre's role is to assist Commander MARCOM in making decisions, deploying forces and coordinating action.[35] The Centre is expected to support Baltic Sentry, a maritime operation launched by NATO in January 2025 to deliver focused deterrence throughout the Baltic Sea in response to recent incidents there.[36]

Third, safeguarding maritime infrastructure requires resilience, which in general terms refers to the ability of a system to resist adverse impacts and to adapt to maintain its essential functions. Resilience can make a key contribution to mitigating vulnerabilities, recovering from the effects of hybrid attacks, and deterring adversaries by denial.[37] To increase their resilience, critical maritime systems need to be hardened against attack. Depending on the assets in question, this may include measures such as implementing stricter access controls to reduce the risk of sabotage, or investing in advanced cybersecurity solutions. Redundancy in critical infrastructure, such as power and communications systems, can help to ensure continuity of operations during disruptions. In addition, resilience also has a legal dimension, concerned with reinforcing the capacity of the applicable legal frameworks and processes to cope with the harms posed by hybrid threats.[38] Adopting a legal resilience perspective encourages coastal states to incorporate all the legal authorities available to them under the law of the sea into their domestic legal systems and to establish processes to exercise those authorities to their full extent.

34 Vilnius Summit Communiqué issued by NATO Heads of State and Government participating in the Meeting of the North Atlantic Council in Vilnius, 11 July 2023, para. 65, https://www.nato.int/cps/ge/natohq/official_texts_217320.htm.

35 MARCOM, 'NATO Officially Launches new Maritime Centre for Security of Critical Undersea Infrastructure', 28 May 2024, https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui.

36 Supreme Headquarters Allied Powers Europe, 'Baltic Sentry to enhance NATO's Presence in the Baltic Sea', 14 January 2025, https://shape.nato.int/news-releases/baltic-sentry-to-enhance-natos-presence-in-the-baltic-sea.

37 U.S. Embassy Maldives, 'Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World', 29 January 2025, https://mv.usembassy.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/.

38 Aurel Sari, 'Hybrid Threats and the Law: Building Legal Resilience', Hybrid CoE Research Report 3 (The European Centre of Excellence for Countering Hybrid Threats, 2021).

3. Legal authorities in the maritime domain

The law of the sea governs the rights and responsibilities of states in the use of the world's oceans. The applicable rules are codified primarily in the United Nations Convention on the Law of the Sea (UNCLOS),[39] adopted in 1982. UNCLOS divides the maritime domain into various jurisdictional zones, each of which confers different sets of rights and responsibilities on coastal and other states, including different sets of enforcement authorities.

Maintaining situational awareness typically involves measures such as the use of radar, which do not impede the movement of foreign vessels or other uses of the sea.[40] By contrast, operational action taken in response to hybrid threats, such as the interdiction of a foreign-flagged vessel, is more likely to interfere with the rights and freedoms enjoyed by other states.[41] Any action that infringes on the rights of other states must have a legal basis in the law of the sea or other applicable legal regimes.[42] As a general rule, only ships in government service may take enforcement action. Moreover, such action may not be directed against foreign vessels that enjoy sovereign immunity, such as warships, other than in circumstances recognized by UNCLOS[43] or in the exercise of the right of self-defence.[44]

The measures that states are entitled to take to safeguard their maritime infrastructure from hybrid threats therefore depend primarily on the type of asset involved, its location in the marine environment, the nature of the measures they intend to adopt and their target. This section provides an overview of the relevant jurisdictional zones and the authorities they confer upon states to maintain situational awareness and to take operational action in response to harmful activities.

3.1 Jurisdictional zones under the law of the sea

The law of the sea seeks to balance the interests of coastal states and other states by creating jurisdictional zones and conferring different sets of rights and responsibilities on states within them.

All waters on the landward side of a coastal state's baseline, which is typically the low-water line along the coast, constitute *internal waters*.[45] This includes ports, bays, rivers, lagoons and lakes. Coastal states exercise full sovereignty over their internal waters in the same way as they do over their land territory, meaning that they may exercise all their legislative and enforcement powers in relation to

39 United Nations Convention on the Law of the Sea, 10 December 1982, 1833 UNTS 3.

40 Cf. *Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua v. Colombia)* (Merits) (2022) ICJ Rep. 266, para. 100 (distinguishing observation carried out by vessels in the EEZ of another state from exercising control).

41 *The M/V 'Norstar' (Panama v. Italy)* (2019) Judgment, 10 April 2019 (International Tribunal for the Law of the Sea), para. 222.

42 *The Arctic Sunrise Arbitration (Netherlands v. Russia)* (2015) Award, 14 August 2015 (Arbitral Tribunal instituted under Annex VII to UNCLOS), para. 222.

43 Article 32, UNCLOS.

44 Article 51, United Nations Charter. See section 4 below.

45 Article 8(1), UNCLOS.

those waters and any events taking place therein.[46] Foreign vessels do not have an automatic right of access to internal waters. Instead, they may enter only at the discretion and with the consent of the coastal state.[47]

The *territorial sea* of a coastal state extends up to 12 nautical miles from its baseline out towards the sea.[48] The territorial sea, together with the airspace above and the seabed and subsoil below, is subject to the exclusive sovereignty of the coastal state.[49] Accordingly, coastal states are entitled to exercise the full range of sovereign powers inside their territorial sea, including all legislative and enforcement authorities, subject to any limits imposed by UNCLOS and other applicable rules of international law.[50] These limits include the right of innocent passage, which entitles foreign vessels to pass through the territorial sea in a continuous and expeditious manner and in a way that is not prejudicial to the peace, good order or security of the coastal state.[51] While coastal states may adopt certain laws and regulations relating to innocent passage, including for the protection of facilities and installations located in the territorial sea,[52] in doing so, they may not impose any requirements on foreign ships which have the practical effect of denying or impairing their right of innocent passage.[53]

The *contiguous zone* extends up to 24 nautical miles from the baseline, encompassing the 12-mile territorial sea and an additional 12 nautical miles of water.[54] The contiguous zone serves as a buffer to enhance the coastal state's ability to ensure compliance with key laws, but without infringing on the freedom of navigation enjoyed by other states. Accordingly, coastal states do not enjoy sovereignty over the contiguous zone, but may exercise the control necessary to prevent violations of their customs, fiscal, immigration or sanitary laws and regulations within their territory or territorial sea and to punish breaches of such laws and regulations committed therein.[55]

Coastal states may establish an *exclusive economic zone* (EEZ) extending up to 200 nautical miles from the baseline.[56] The role of the EEZ is to reconcile the traditional freedom of navigation with the growing demand of coastal states to control and exploit the natural resources of the sea. Within the EEZ, coastal states enjoy three sets of rights. First, they hold sovereign rights for the purpose of exploring, exploiting, conserving and managing the natural resources of the waters, the seabed and the subsoil, and to carry out other activities for the economic exploitation and exploration of the zone, including energy production.[57] Second, they may exer-

46 Article 2(1), UNCLOS.
47 *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA)*, (Merits) (1986) ICJ Rep. 14, para. 213.
48 Article 3, UNCLOS.
49 Articles 2(1) and 2(2), UNCLOS.
50 Yoshifumi Tanaka, *The International Law of the Sea* (Cambridge: Cambridge University Press, 2012), 104.
51 Articles 17–19, UNCLOS.
52 Article 21, UNCLOS.
53 Article 24, UNCLOS.
54 Article 33(2), UNCLOS.
55 Article 33(1), UNCLOS.
56 Article 57, UNCLOS.
57 Article 56(1)(a), UNCLOS.

cise jurisdiction as provided for in UNCLOS with regard to the establishment and use of artificial islands, installations and structures, marine scientific research and the protection and preservation of the marine environment.[58] Finally, they may also regulate certain other matters, such as dumping and vessel-borne pollution.[59] However, other states retain broad freedoms in the EEZ, particularly the freedom of navigation and overflight, as well as the right to lay submarine cables and pipelines.[60]

The *continental shelf* comprises the seabed and subsoil of a coastal state's submarine areas extending beyond its territorial sea as a natural prolongation of its land territory, up to 200 nautical miles or further if the prolongation of the landmass extends beyond that distance, subject to certain limits.[61] Coastal states have exclusive sovereign rights over the continental shelf for the purposes of exploring and exploiting its natural resources.[62] However, these rights do not affect the legal status of the waters above the continental shelf and their exercise must not infringe upon, or result in any unjustifiable interference with, navigation and other freedoms enjoyed by other states.[63] In addition, all states are entitled to lay submarine cables and pipelines on the continental shelf.[64]

The *high seas* begin beyond the EEZ and are open to all states, whether coastal or landlocked.[65] The high seas are not subject to sovereignty or national jurisdiction.[66] Instead, they are governed by the principle of freedom of the seas, which allows states to engage in navigation, overflight, laying submarine cables and pipelines, the construction of artificial islands and other installations, fishing and scientific research.[67] The seabed and subsoil beyond national jurisdiction, referred to as '*the Area*', are not subject to sovereignty or sovereign rights either, but are designated as the 'common heritage of mankind', administered by the International Seabed Authority under UNCLOS.[68]

Straits and archipelagic waters present unique challenges due to their dual nature: they form parts of the territorial sea or the internal waters of coastal or archipelagic states, yet they are also used for international navigation. UNCLOS defines international straits as natural passages between two parts of the high seas or EEZs used for international shipping.[69] Ships and aircraft of all states enjoy the right of transit passage through such straits, meaning that they may navigate continuously and expeditiously without being impeded by the coastal state.[70] Although coastal states have sovereignty over

58 Article 56(1)(b), UNCLOS.
59 Article 56(1)(c), UNCLOS, in conjunction with Articles 210(5) and 211(5), UNCLOS.
60 Article 58, UNCLOS.
61 Article 76, UNCLOS.
62 Article 77, UNCLOS.
63 Article 78, UNCLOS.
64 Article 79, UNCLOS.
65 Article 86, UNCLOS.
66 Article 89, UNCLOS.
67 Article 87, UNCLOS.
68 Articles 136–137, UNCLOS.
69 Article 37, UNCLOS.
70 Article 38, UNCLOS.

the territorial sea that forms part of a strait, their ability to regulate transit passage is limited to certain specific matters, such as the safety of navigation and the prevention of pollution.[71] The passage through straits regulated by long-standing international conventions, such as the Danish Belts and the Sound, is governed by those conventions.[72] Finally, archipelagic states may designate specific sea lanes and air routes for continuous and expeditious passage by foreign ships and aircraft, known as archipelagic sea lanes passage.[73]

3.2 Maintaining situational awareness

Since the sovereignty of coastal states extends to their internal waters and territorial sea, they enjoy broad powers to gather information in these zones, subject to the rights and freedoms enjoyed by other states. For instance, coastal states may decide to admit foreign ships into their internal waters on condition that they comply with certain reporting requirements. Inside their territorial waters, coastal states may impose mandatory reporting requirements on foreign vessels in the exercise of their right to adopt laws and regulations with respect to the safety of navigation and the regulation of maritime traffic.[74] For example, these arrangements may take the form of vessel traffic services (VTS) to receive, process and share navigational and other information between the coastal state and maritime traffic.[75]

In addition, coastal states may take the necessary steps in their territorial sea to prevent passage which is not innocent. This necessarily implies the right to collect information to determine whether the passage of foreign vessels is innocent or not.[76] Beyond receiving and collecting information to ensure the safety of navigation and to regulate maritime traffic, coastal states therefore enjoy a more general right in their territorial sea to gather information necessary to safeguard their peace, good order and security.[77]

The right to maintain maritime awareness in jurisdictional zones not subject to sovereignty may be based on three principles. First, specific rights conferred by UNCLOS imply an authority to engage in information-gathering activities to the extent necessary to exercise those rights

71 Article 42, UNCLOS. In addition, the right of innocent passage applies to straits used for international navigation which are not subject to the regime of transit passage, pursuant to Article 45, UNCLOS.

72 Article 35(c), UNCLOS.

73 Article 53, UNCLOS.

74 International Convention for the Safety of Life at Sea, 1 November 1974, (consolidated), Chapter V, Regulation 12(3).

75 Para 3(1), International Maritime Organization, Guidelines for Vessel Traffic Services, Resolution A.1158(32), 15 December 2021. See Anish Arvind Hebbar, Jens-Uwe Schröder-Hinrichs and Serdar Yildiz, 'Vessel Traffic Management in the Era of Maritime Autonomous Surface Ships and Digitalization: Experiences in European Waters', in *Area-Based Management of Shipping: Canadian and Comparative Perspectives*, ed. Aldo Chircop, et al. (Cham: Springer, 2024), 185–205, 187–190.

76 Article 25, UNCLOS.

77 Cf. *Dispute concerning Delimitation of the Maritime Boundary between Ghana and Côte d'Ivoire in the Atlantic Ocean (Ghana/Côte d'Ivoire), Provisional Measures* (2015) Order, 25 April 2015 (International Tribunal for the Law of the Sea), para. 94.

effectively.[78] For instance, coastal states must be free to gather information in order to determine whether it is necessary to exercise control in their contiguous zone to prevent infringements of their customs, fiscal, immigration or sanitary laws within their territory or territorial sea. Similarly, states must be able to gather any information required to exercise their rights in an EEZ or on the high seas. For example, all states are bound under UNCLOS to cooperate in the repression of piracy on the high seas and may seize pirate ships or aircraft on suspicion of piracy.[79] States must be free to collect information to confirm suspicions they may harbour that a particular ship or aircraft is engaged in piracy, since seizure without adequate grounds renders them liable to compensate the state of nationality for any loss or damage caused by the seizure.[80]

Second, an authority to maintain situational awareness may be considered implicit in the freedom of navigation and the freedom of the seas more generally, subject to the principle of due regard for the rights and duties of other states and any specific restrictions imposed by UNCLOS.[81] The existence of such an authority may be deduced from the regime of innocent passage. Under that regime, the passage of a foreign ship through the territorial sea does not qualify as innocent if the vessel engages in any act aimed at collecting information to the prejudice of the defence or security of the coastal state.[82] This suggests not only that foreign vessels passing through the territorial sea are free to gather information for other purposes,[83] provided these are not prohibited,[84] but also that they may engage in information gathering outside the territorial sea in the exercise of the freedom of navigation, bearing in mind that the restrictions imposed by the innocent passage regime do not apply to navigation outside territorial waters.

Third, if states are entitled to undertake military intelligence-gathering activities in the EEZ of other nations,[85] as well as on the high seas, it stands to reason that they must also be entitled to collect information in those zones through non-military means and methods.

78 Cf. *Corfu Channel Case (Albania v. UK)*, (Merits) (1949) ICJ Rep. 4, 18–22 (taking for granted that a coastal state has the right to monitor and observe activities prejudicial to its sovereignty taking place in its territorial waters).

79 Article 105, UNCLOS.

80 Article 106, UNCLOS.

81 Cf. James Kraska, 'Intelligence Collection and the International Law of the Sea', *International Law Studies*, Volume 99 (2022): 602–637, 605–617.

82 Article 19(2)(c), UNCLOS.

83 Stuart B. Kaye, 'Freedom of Navigation, Surveillance and Security: Legal Issues Surrounding the Collection of Intelligence from Beyond the Littoral', *Australian Yearbook of International Law*, Volume (2005): 93–105, 96.

84 E.g. information gathering for the purpose of conducting research or survey activities would not be compatible with Article 19(2)(j), UNCLOS.

85 See Natalie Klein, *Maritime Security and the Law of the Sea* (Oxford: Oxford University Press, 2011), 219–221; Moritaka Hayashi, 'Military and Intelligence Gathering Activities in the EEZ: Definition of Key Terms', *Marine Policy*, Volume 29 (2005): 123–137.

3.3 Taking operational action

As a preliminary point, it is useful to distinguish between two categories of operational action that states may take in response to maritime hybrid threats: law-enforcement measures involving the exercise of enforcement jurisdiction in response to a suspected violation of the applicable law, such as boarding and arresting a foreign vessel; and preventive or protective measures to safeguard a state's rights and interests against unlawful interference or harm, such as compelling a vessel engaged in non-innocent passage to leave the territorial sea.[86]

Since coastal states enjoy sovereignty over their internal waters and territorial sea, they are entitled to enforce their laws and regulations in these zones. Provided they have adopted domestic legislation to criminalize acts directed against maritime infrastructure, they may enforce those rules against foreign vessels suspected of violating them, including by boarding, inspecting and searching the vessels concerned, by arresting them or the persons on board, or by seizing their cargo. However, to safeguard the interests of other states, Article 27 UNCLOS provides that coastal states 'should not' exercise their criminal jurisdiction on board a foreign ship passing through the territorial sea, except in certain circumstances.[87] Two of these are relevant in the context of hybrid threats: situations where the consequences of the alleged crime extend to the coastal state, and situations where the alleged crime is of a kind to disturb the peace of the country or the good order of the territorial sea.[88] By definition, hybrid threat activities directed against critical maritime infrastructure are likely to fall into one or both of these categories.[89] This means that Article 27 UNCLOS is therefore unlikely to prevent coastal states from exercising their enforcement jurisdiction against vessels suspected of engaging in hybrid threat activities within their territorial sea.

In addition, coastal states may also exercise enforcement powers against vessels that fail to comply with their laws and regulations relating to innocent passage, including rules concerning the protection of facilities, installations, cables and pipelines.[90] Even though the existence of such enforcement powers is not expressly recognized by UNCLOS, it would make little sense to accept that coastal states may regulate certain aspects of innocent passage without accepting that they may enforce those rules.

Pursuant to Article 25 UNCLOS, coastal states may also take the necessary steps in their territorial sea to prevent passage which is not innocent. What action is necessary to prevent non-innocent passage depends on the circumstances. It is understood that it may include measures to compel a delinquent vessel to

86 Cf. *Arctic Sunrise*, para. 306.

87 This is generally understood as 'hortatory', rather than as an absolute prohibition of exercising criminal jurisdiction other than for the purposes listed in Article 27. See Richard Barnes, 'Article 27', in *United Nations Convention on the Law of the Sea: A Commentary*, ed. Alexander Proelss (München: C. H. Beck, 2017), 229–237, 233–234; *Pianka v. R.* [1979] A.C. 107, 125.

88 Articles 27(1)(a) and 27(1)(b), UNCLOS.

89 Cf. Christian Schaller, 'Russia's Mapping of Critical Infrastructure in the North and Baltic Seas: International Law as an Impediment to Countering the Threat of Strategic Sabotage?', *Nordic Journal of International Law*, Volume 93 (2024): 202–236, 209–210.

90 Articles 21(1)(b) and 21(1)(c), UNCLOS.

leave the territorial sea, including by the use of proportionate force, if necessary.[91] In addition to expelling vessels, there is no reason why coastal States may not block or otherwise restrict their movements if the circumstances so require, for example to prevent them from causing damage to critical infrastructure.

In the contiguous zone, coastal states may take enforcement action, but only in relation to the infringement of their customs, fiscal, immigration or sanitary laws and regulations.[92] This is an exhaustive list. In the present context, its relevance is limited, since in most circumstances hybrid activities directed against maritime infrastructure are unlikely to engage customs, fiscal, immigration or sanitary laws and regulations, except perhaps in an incidental manner.[93]

In their EEZ, coastal states may exercise enforcement jurisdiction in relation to their sovereign rights to explore, exploit, conserve and manage the natural resources of the EEZ. Article 73 UNCLOS entitles coastal states to ensure compliance with the laws and regulations they have adopted in relation to the EEZ's living resources. No provision in UNCLOS authorizes corresponding enforcement measures in relation to non-living resources. However, such an authority is understood to exist under customary international law,[94] as recognized by the arbitral tribunal in the *Arctic Sunrise* case.[95] Where hybrid threats directed against maritime infrastructure violate coastal state laws and regulations in relation to the EEZ's natural resources, the relevant coastal states may exercise enforcement jurisdiction in response to those threats, for instance in the form of boarding, inspection, arrest and judicial proceedings.

In the *Arctic Sunrise* case, the arbitral tribunal held that coastal states are also entitled to take certain measures to prevent interference with their sovereign rights for the exploration and exploitation of the EEZ's non-living resources.[96] The tribunal declared that it 'would be reasonable for a coastal state to act to prevent: (i) violations of its laws adopted in conformity with the Convention; (ii) dangerous situations that can result in injuries to persons and damage to equipment and installations; (iii) negative environmental consequences [...]; and (iv) delay or interruption in essential operations'.[97] In addition, the tribunal recognized the existence of a distinct right for coastal states to take preventive action against a vessel reasonably believed to be involved in a terrorist attack on their installations or structures in the EEZ.[98] Separately, coastal states are permitted to establish

91 I. A. Shearer, 'Problems of Jurisdiction and Law Enforcement Against Delinquent Vessels', *International and Comparative Law Quarterly*, Volume 35 (1986): 320–343, 325.

92 Article 33, UNCLOS.

93 In this context, it is important to underline that 'sanitary' rules cannot simply be equated with rules relating to pollution. *Cf.* Daniel-Erasmus Khan, 'Article 33', in *United Nations Convention on the Law of the Sea: A Commentary*, ed. Alexander Proelss (München: C. H. Beck, 2017), 254–271, 267.

94 Cf. Tanaka, *The International Law of the Sea*, 172.

95 *Arctic Sunrise*, para. 284.

96 Ibid., para. 324.

97 Ibid., para. 327. Although the tribunal's decision is limited to interference caused by 'protest action', the underlying principle, which is the coastal state's right to safeguard its sovereign rights from interference, is broader in scope.

98 Ibid., para. 314.

safety zones around artificial islands, installations and structures, not exceeding a distance of 500 metres around them, and to take appropriate measures to ensure their safety within those zones.[99]

Coastal states also enjoy certain powers for the protection and preservation of the marine environment.[100] However, not all of these are equally relevant in the context of hybrid threats. Pursuant to Article 220 UNCLOS, coastal states may exercise their enforcement jurisdiction in relation to pollution from vessels. Even though deliberate attacks against certain maritime assets, such as oil rigs or pipelines, may release harmful substances that could cause significant levels of pollution, this would not constitute pollution *from vessels* and therefore falls outside the scope of Article 220. By contrast, Article 221 UNCLOS entitles coastal states to take and enforce measures beyond the territorial sea to protect their coastline or related interests, including fishing, from pollution or the threat of pollution following a 'maritime casualty'[101] that may reasonably be expected to result in major harmful consequences. In principle, a collision between a vessel and a piece of critical maritime infrastructure could engage this rule, but a coastal state would be entitled to take enforcement action only if necessary to protect its coastline and related interests from pollution or the threat of pollution. In other words, the scope of its enforcement authority under this provision is limited.

On the continental shelf, coastal states may take reasonable measures to prevent, reduce and control pollution from submarine pipelines. However, this right is related to their duty not to impede the laying or maintenance of submarine cables or pipelines by other states.[102] The measures a coastal state is entitled to take in this context therefore seem to be limited to preventing, reducing and controlling pollution from the laying, maintenance and operation of submarine pipelines by other states, without extending to pollution that foreign vessels may cause by damaging such pipelines.[103]

On the high seas, flag-state jurisdiction is the primary basis for the exercise of enforcement powers over ships.[104] Although some of the rules discussed, such as Article 221 UNCLOS, extend to the high seas, any enforcement authority they confer in relation to hybrid threats remains limited. In addition, states may exercise enforcement powers over certain universally

99 Articles 60(4) and 60(5), UNCLOS.

100 Article 56(1)(b)(iii), UNCLOS.

101 For the purposes of this rule, a 'maritime casualty' refers to 'a collision of vessels, stranding or other incident of navigation, or other occurrence on board a vessel or external to it resulting in material damage or imminent threat of material damage to a vessel or cargo', as defined in Article 221(2), UNCLOS.

102 Article 79(2), UNCLOS.

103 Cf. Martha M. Roggenkamp, 'Petroleum Pipelines in the North Sea: Questions of Jurisdiction and Practical Solutions', *Journal of Energy and Natural Resources Law*, Volume 16 (1998): 92–109, 106. For a different position, see Sarah Wolf, *Unterseeische Rohrleitungen und Meeresumweltschutz: Eine völkerrechtliche Untersuchung am Beispiel der Ostsee* (Heidelberg: Springer, 2011), 231. See also Schaller, 'Russia's Mapping of Critical Infrastructure', 230–232.

104 Article 92(1), UNCLOS.

recognized crimes, including piracy,[105] slavery,[106] and unauthorized broadcasting.[107] Among these, piracy is the most relevant in the context of hybrid threats. Certain international conventions also provide for the exercise of enforcement jurisdiction by one state party against vessels flying the flag of another. Under the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, a state party which suspects that a vessel flying the flag or displaying marks of registry of another party is engaged in illicit traffic may notify the flag state and request authorization to take appropriate measures, including boarding, searching or other appropriate action with respect to the vessel, persons, or cargo if evidence of involvement in illicit traffic is found.[108] Similar arrangements are made in the Protocol against the Smuggling of Migrants by Land, Sea and Air to the United Nations Convention against Transnational Organized Crime.[109]

105 Article 105, UNCLOS.
106 Article 110(1)(b), UNCLOS.
107 Article 110(1)(c), UNCLOS.
108 Article 17, United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 20 December 1988, 1582 UNTS 165.
109 Article 8(2), Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, 15 November 2000, 2241 UNTS 507.

4. Countering hybrid threats more effectively

The authority of states to safeguard critical maritime infrastructure against hybrid threats is based on a patchwork of rules under the law of the sea. Generally, the authority of coastal states to take action against foreign vessels is at its broadest inside their internal and territorial waters and at its weakest on the high seas, where the exclusive jurisdiction of the flag state dominates.

This zonal logic of the law of the sea may be appropriate for balancing the interests of coastal and other states when it comes to navigational rights and the exploitation of natural resources, but it does not sit well with the character and vulnerabilities of some categories of maritime infrastructure. For example, submarine communication cables connecting distant shores may cross from the territorial sea of one coastal state into the high seas and back into the territorial waters of another coastal state. As a practical matter, it makes little difference whether such cables are deliberately cut inside territorial waters or on the high seas. The effect is the same: their operations will be interrupted. States relying on the services provided by submarine cables have a legitimate interest in protecting them from deliberate attack regardless of where it occurs, yet the law of the sea grants them few powers to do so outside their territorial waters.[110] Indeed, this gap in the law presents a vulnerability that hostile actors may be tempted to exploit.

This section assesses the legal authorities available to counter maritime hybrid threats, identifying key gaps before focusing on the protection of submarine communication cables in more detail and on the implications of the rules governing the use of force.

4.1 Jurisdictional zones: what falls between the gaps?

The law of the sea confers broad authorities on states to maintain situational awareness in the maritime domain as part of their efforts to counter hybrid threats. Coastal states enjoy extensive rights to gather information in their internal waters and territorial sea. In other zones, all states benefit from an implicit authority to maintain situational awareness where this is necessary to exercise specific rights conferred upon them by UNCLOS or to comply with their obligations, such as the duty to cooperate in the suppression of piracy. For example, the sovereign right to economic exploitation of the EEZ entitles coastal states to construct and operate offshore wind farms. This necessarily implies the power to gather information to ensure the continued operation of these installations and to safeguard their security, for instance by monitoring maritime traffic and other activi-

110 Cf. Henrik Ringbom and Alexander Lott, 'Sabotage of Critical Offshore Infrastructure: a Case Study of the Balticconnector Incident', in *Maritime Security Law in Hybrid Warfare*, ed. Alexander Lott (Leiden: Brill, 2024), 155–194, 177 (suggesting that it would defeat the purpose of UNCLOS 'if a ship were free to engage in illegal activities that are blatantly against the interest of the majority of states in protecting submarine critical infrastructure and especially those of the coastal state in its own EEZ, without offering the state which suffers considerable damage from the act of sabotage any opportunity to intervene'). Generally, see Douglas R. Burnett, 'Submarine Cable Security and International Law', *International Law Studies*, Volume 97 (2021): 1659–1682.

ties nearby.[111] Similarly, since the freedom to lay submarine cables and pipelines on the high seas includes the right to operate and maintain them,[112] this freedom also implies the power to gather information necessary for their continued functioning and security. In principle, the right to gather information is not limited to the use of any specific asset, but may involve shore-based installations, ships, aircraft, underwater vehicles and sensors, other maritime systems and space-based assets.

In waters not subject to sovereignty, states may employ ships and aircraft in government service to gather information in the exercise of the freedom of navigation and overflight. They may deploy such ships and aircraft to monitor the activities of foreign vessels, provided that in doing so they respect their rights and freedoms under UNCLOS and other applicable rules of international law. A recent example of such information gathering is the monitoring of *Yi Peng 3*, the Chinese-registered vessel suspected of severing communication cables in the Baltic Sea in November 2024, by Danish, German, and Swedish coast guard and navy vessels.[113]

Overall, the law of the sea provides states with sufficient legal authorities to maintain comprehensive situational awareness, leaving no significant gaps in their ability to carry out monitoring, surveillance and information gathering. Given that such activities typically do not involve physical interference with foreign vessels or other uses of the sea, they are unlikely to infringe on the rights of other states and elicit objections on this basis. States displeased with information-gathering activities conducted by other nations are more likely to characterize them as intelligence collection prejudicial to their security and denounce them as incompatible, for instance, with the regime of innocent passage.[114] However, as long as EU and NATO member states do not deploy assets to gather information inside the territorial sea and the EEZ of unfriendly or uncooperative states, no such objections should materialize.

The picture is different when it comes to the legal bases for taking operational action. The law of the sea contains few rules specifically designed to protect critical maritime infrastructure against malign interference and deliberate harm. Express legal authorities, such as the right of coastal states to establish safety zones around artificial islands, installations and structures they have constructed in their EEZ, are the exception. The absence of rules systematically protecting maritime infrastructure is a significant blind spot in the legal regime of the oceans.[115]

111 An alternative basis for such information gathering is Article 60(4), UNCLOS, which authorizes coastal states to establish reasonable safety zones around their artificial islands, installations and structures within which they may take appropriate measures to ensure the safety of navigation and of such artificial islands, installations and structures.

112 International Law Association, Committee on Submarine Cables and Pipelines under International Law, 'First Interim Report', 2020, 7–8.

113 Michael Schwirtz, Muyi Xiao and Riley Mellen, 'EU Vessels Surround Anchored Chinese Ship After Baltic Sea Cables are Severed', *The New York Times*, 27 November 2024, https://www.nytimes.com/2024/11/27/world/europe/baltic-sea-cables-chinese-ship.html.

114 See Kraska, 'Intelligence Collection', 610–625.

115 Cf. Christian Bueger, 'Maritime Security in the Age of Infrastructure', *ASCOMARE Yearbook on the Law of the Sea*, Volume 3 (2023): 73–88, 76–77.

This is less of a problem for coastal states inside their internal waters and within their territorial sea. As we have seen, the exercise of enforcement jurisdiction in response to hybrid activities is likely to fall within the scope of the permissible exercises of criminal jurisdiction under Article 27 UNCLOS. Moreover, since the passage of foreign vessels engaged in malign activities is unlikely to qualify as innocent, coastal states may take appropriate action against them. However, beyond these zones, efforts to safeguard critical maritime infrastructure must rely on legal authorities that were designed to address different matters and which may apply to maritime infrastructure only indirectly.

In some cases, it is difficult to see how hybrid threat activities might fall within the scope of the enforcement powers available in zones beyond national sovereignty. For example, enforcement measures in the contiguous zone are limited to the infringement of customs, fiscal, immigration or sanitary laws and regulations.[116] It is unlikely that hybrid threats against maritime infrastructure would implicate such laws and regulations. The same is true for the authority to exercise enforcement jurisdiction in relation to pollution from vessels.[117]

In other cases, there might be a better fit. For instance, hybrid threat activities are more likely to violate some of the laws and regulations a coastal state has adopted in relation to the exploration, exploitation, conservation and management of the natural resources of the EEZ, thus triggering its right to take measures necessary to enforce compliance with those rules. In the *M/V 'Virgina G'* case, the International Tribunal for the Law of the Sea held that coastal states are entitled to regulate the bunkering of foreign vessels engaged in fishing in their EEZ, on the basis that fishing in the EEZ is one of the sovereign rights to which coastal states may extend their laws in accordance with UNCLOS, and that the supply of fuel is a supporting activity directly connected to fishing.[118] The same logic applies to other sovereign rights. Since coastal states are entitled to apply their domestic laws on property ownership to the resources and assets located in the EEZ,[119] it would not be unreasonable if they extended the application of other domestic rules relevant to property, such as their rules of criminal and civil law protecting property against theft or damage to assets in their EEZs. If they were to do so, hybrid threat activities causing damage to maritime infrastructure would likely be caught by these laws, which in turn would entitle coastal states to take action necessary to enforce compliance, for instance by interdicting and possibly arresting the foreign vessels involved.

However, it should be underlined that coastal states may extend their domestic laws pursuant to Article 73 UNCLOS only to matters that are directly or closely related to the exercise of their sovereign rights in the EEZ. Similarly, any exercise of enforcement powers is permissible only if necessary to secure compliance with

116 Article 33, UNCLOS.

117 Article 221, UNCLOS.

118 *The M/V 'Virginia G' Case (Panama/Guinea-Bissau)* (2014) Judgment, 14 April 2014 (International Tribunal for the Law of the Sea), paras 208–219.

119 Catherine Redgwell, 'Property Law Sources and Analogies in International Law', in *Property and the Law in Energy and Natural Resources*, ed. Aileen McHarg et al. (Oxford University Press, 2010), 100–112, 109–110.

those rules, either to punish offenders or to deter other vessels from breaking the law,[120] and must be based on reasonable grounds.[121] The more tenuous the link between hybrid threats on the one side and the regulation of sovereign rights and the need to secure compliance with those rules on the other, the less compelling the exercise of prescriptive and enforcement jurisdiction will be. It is reasonable to expect that other states, including Russia, would object to the exercise of jurisdiction that does not fall squarely within the parameters of UNCLOS and would take measures in response.[122] It should also be emphasized that the limited nature of these jurisdictional powers means that they do not cover certain types of assets at all. The most glaring gap concerns submarine communication cables that run through the EEZ without servicing any artificial islands, installations and structures constructed there.

The principle announced in the *Arctic Sunrise* case entitles coastal states to take operational action against hybrid threat activities that interfere with or threaten to infringe on the exercise of their sovereign rights in the EEZ. This goes a long way towards enabling coastal states to react promptly to ongoing incidents.[123] For example, it entitles coastal states to take appropriate measures against vessels to stop or prevent them from causing damage to wind farms or similar installations in the EEZ, or from interrupting the operation of such installations. Coastal states could also rely on the principle to visit and search vessels suspected of posing such a threat. The *MV Ruby* incident is a case in point. The *MV Ruby*, a Maltese-flagged cargo vessel, suffered significant storm damage after leaving a Russian port in July 2024, carrying a substantial amount of ammonium nitrate. The ship was denied permission to dock for repairs by several European countries due to safety and environmental concerns about its cargo.[124] Had the *MV Ruby* failed to cooperate with coastal states or concealed its intentions, interdiction may have been necessary and could have been justified pursuant to the *Arctic Sunrise* principle. Although not expressly confirmed by the tribunal, the principle would also seem to entitle coastal states to take preventive or protective action against hybrid threat activities directed against any artificial islands, installations and structures they have constructed in their EEZ for the exploitation of its natural resources.[125]

However, the *Arctic Sunrise* principle does not cover the protection of cables, pipelines or other assets that do not exploit the natural resources of the EEZ, but merely run through it. Nor does it entitle a coastal state to exercise

120 *The M/V 'Virginia G' Case*, para. 269.

121 Cf. James Harrison, 'Safeguards against Excessive Enforcement Measures in the Exclusive Economic Zone–Law and Practice', in *Jurisdiction over Ships: Post-UNCLOS Developments in the Law of the Sea*, ed. Henrik Ringbom (Leiden: Brill, 2015), 217–248, 221–222.

122 Cf. Østhagen, 'The Arctic After Russia's Invasion of Ukraine', 12–13.

123 But see Brian Wilson, 'Advancing the Law of Vessel Interference by Non-State Actors', *Texas International Law Journal*, Volume 55 (2019): 159–186, 177 (suggesting that the categories of action that may be regarded as interference with the exercise of sovereign rights are incomplete).

124 Matt Precey, 'How an Explosion-risk Ship ended up in Norfolk', BBC, 22 November 2024, https://www.bbc.co.uk/news/articles/c2062g4dzwro; Joshua Cheetham and Amy Walker, 'Ship Carrying Explosive Fertiliser heads to UK Waters', BBC, 26 September 2024, https://www.bbc.co.uk/news/articles/c62g95721leo.

125 This would be in addition to the powers set out in Article 60, UNCLOS.

its enforcement jurisdiction where no separate basis for doing so already exists. Thus, a coastal state may invoke the principle to intercept a foreign vessel dragging its anchor towards a submarine cable that connects an offshore wind farm in its EEZ to shore-based installations in order to prevent the cable from being damaged, but it cannot rely on the principle to board, search and arrest the same vessel in its EEZ after it has already severed the cable.[126]

It seems that these limitations did not prevent the Finnish authorities from boarding and taking control of the *Eagle S*, a Cook Islands-flagged tanker, on 26 December 2024, after the vessel severed the Estlink 2 power cable running between Finland and Estonia, together with several submarine communication cables.[127] The *Eagle S* was subsequently escorted into Finnish territorial waters and seized.[128] It is unclear at this point on what legal basis the Finnish authorities acted.[129] The *Artic Sunrise* principle does not seem to apply here, as the Estlink 2 cable merely transits Finland's EEZ, without exploiting its natural resources. Concerns have been expressed that the *Eagle S* might cause an oil spill. Pursuant to Article 220(6) UNCLOS, Finland would be entitled to institute proceedings against the *Eagle S* under its domestic law, which may include detaining the vessel, if it had 'clear objective evidence' that the ship had committed a violation of the applicable international rules and standards for preventing, reducing and controlling pollution from vessels, and that such a violation resulted in a 'threat of major damage to the coastline or related interests' of Finland. No such 'clear objective evidence' has been presented. Instead, the Finnish authorities have opened an investigation on suspicion of 'aggravated criminal mischief' and 'aggravated interference of communications'.[130] This suggests that they are not relying on Article 220 UNCLOS.

If the Finnish authorities interdicted the *Eagle S* without legal authority, this could amount to an interference with the flag state's freedom of navigation. However, Finland may be able to rely on Article 25 of the Articles on State Responsibility to invoke necessity as a circumstance precluding the wrongfulness of its actions.[131] Pleading necessity could enable

126 Cf. Joanna Mossop, 'Protests against Oil Exploration at Sea: Lessons from the Arctic Sunrise Arbitration', *International Journal of Marine and Coastal Law*, Volume 31 (2016): 60–87, 73.

127 Yle, 'Estlink Cable Disruption: Finnish Border Guard detains Tanker linked to Russia's 'Dark Fleet', 26 December 2024, https://yle.fi/a/74–20133516.

128 On 3 January 2025, the Helsinki District Court rejected a plea by the tanker's operator to release the vessel. See *Helsinki Times*, 'Finnish Court Denies Release of Tanker in Undersea Cables Investigation', 3 January 2025, https://www.helsinkitimes.fi/finland/finland-news/domestic/25932-finnish-court-denies-release-of-tanker-in-undersea-cables-investigation.html.

129 The Baltic Sentinel, 'Swift Action by Finnish Authorities Prevented Cable-Sabotaging Tanker from Damaging Balticconnector Pipeline', 28 December 2024, https://balticsentinel.eu/8162178/swift-action-by-finnish-authorities-prevented-cable-sabotaging-tanker-from-damaging-balticconnector-pipeline.

130 Police of Finland, 'Cable Ruptures also Investigated as Offences of Aggravated Interference of Communications', 30 December 2024, https://poliisi.fi/en/-/cable-ruptures-also-investigated-as-offences-of-aggravated-interference-of-communications.

131 Article 25, International Law Commission, Draft Articles on the Responsibility of States for Internationally Wrongful Acts with Commentaries, UN Doc. A/56/10 (2001).

Finland to justify its interference with the flag state's rights and hence render it lawful.[132] However, a number of conditions must be satisfied: the interference (a) must have been the only way for Finland to safeguard an essential interest against a grave and imminent peril; and (b) it must not have seriously impaired an essential interest of the state or states towards which the obligation exists, or of the international community as a whole.[133] These conditions are strict.[134] Where a foreign-flagged vessel is in the process of harming maritime infrastructure, as in the present case, the imminence requirement will be satisfied and intercepting the vessel is likely to be the 'only way' for the coastal state to respond to the peril. The key question, therefore, will be whether the peril was sufficiently 'grave' and whether it threatened an 'essential interest'. These conditions may be satisfied where, for example, the damage to a submarine power cable is likely to disrupt essential services with particularly severe economic, safety and security consequences at the national level. In such a situation, interference with the flag state's freedom of navigation would appear to be both reasonable and proportionate. However, where the threat posed to maritime infrastructure is of lesser magnitude, it is unlikely that coastal states would be successful in relying on necessity as a circumstance precluding wrongfulness.

Overall, the legal authorities available to coastal states enable them to exercise enforcement jurisdiction and to take preventive and protective measures in relation to a wide range of maritime facilities, particularly those serving shipping, energy production, fishing and the marine ecosystem, provided that these assets are either located in their territorial waters or connected to the exercise of sovereign and jurisdictional rights in their EEZ. By contrast, their authorities are less extensive when it comes to safeguarding assets located beyond territorial waters that are not closely connected to the exercise of sovereign or jurisdictional rights. Communication infrastructure is a prime example of such assets.

4.2 Submarine communication cables

The limited authority of coastal states to protect submarine communication cables was highlighted by the incident involving the *Yi Peng 3*, a Chinese-flagged bulk carrier, in November 2024. The vessel departed the Russian port of Ust-Luga on 15 November 2024, heading into the Baltic Sea. It is suspected to have severed the BCS East West Interlink communication cable running between Lithuania and Sweden on 17 November, and is believed to have cut the C-Lion1 data communication cable between Finland and Germany on 18 November. Both incidents occurred in Sweden's EEZ.

Preliminary investigations suggested that the *Yi Peng 3* may have dragged its anchor over a distance exceeding 100 miles, eventually severing the two submarine cables, and that

132 On the effect of circumstances precluding wrongfulness, see Federica Paddeu, 'Clarifying the Concept of Circumstances Precluding Wrongfulness (Justifications) in International Law', in *Exceptions in International Law*, ed. Lorand Bartels and Federica Paddeu (Oxford University Press, 2020), 203–224.

133 In addition, necessity may not be invoked if (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the state has contributed to the situation of necessity. Both of these conditions appear to be satisfied here.

134 James Crawford, *State Responsibility: The General Part* (Cambridge: Cambridge University Press, 2013), 305–315.

this may have been a deliberate act. These suspicions were seemingly confirmed by reports that the *Yi Peng 3* had engaged in similar action earlier in 2024, although it failed to cause any damage on that occasion.[135] In a joint statement issued on 18 November, Finland and Germany expressed their deep concern over the incident, noting that 'European security is not only under threat from Russia's war of aggression against Ukraine, but also from hybrid warfare by malicious actors'.[136] A similar statement was issued by the Lithuanian and Swedish defence ministers the following day.[137] Other reports went further, suggesting that the Russian authorities may have been involved, although Kremlin representatives dismissed these suggestions as 'absurd'.[138]

Following the incident, the *Yi Peng 3* entered Denmark's EEZ, where it remained. Investigations were subsequently launched by Denmark, Finland, Germany, Lithuania and Sweden. In Finland, the National Bureau of Investigation opened a criminal investigation on suspicion of 'aggravated criminal mischief and aggravated interference with communications'.[139] Later, in November 2024, Sweden formally requested China to cooperate with its investigation and to help clarify what had happened.[140] In response, China indicated its readiness to work with the relevant countries[141] and on 19 December allowed representatives from Denmark, Finland, Germany and Sweden to board the *Yi Peng 3* to observe a Chinese investigation conducted on board.[142] The ship left the Danish EEZ on 21 December 2024.

135 Jordan King and John Feng, 'Chinese Ship May Have Tried to Sabotage Undersea Cables Before', *Newsweek*, 18 December 2024, https://www.newsweek.com/chinese-ship-yi-peng-3-undersea-cables-damage-2002637.

136 German Federal Foreign Office, Joint Statement by the Foreign Ministers of Finland and Germany on the Severed Undersea Cable in the Baltic Sea, 18 November 2024, https://www.auswaertiges-amt.de/en/newsroom/news/2685132–2685132.

137 Swedish Ministry of Defence, Statement regarding Damaged Communications Cable by the Swedish and Lithuanian Ministers for Defence, 19 November 2024, https://www.government.se/press-releases/2024/11/statement-regarding-damaged-communications-cable-by-the-swedish-and-lithuanian-ministers-for-defence/.

138 Johan Ahlander, 'Danish Military says It's Staying close to Chinese Ship after Data Cable Breaches', 20 November 2024, Reuters, https://www.reuters.com/world/europe/kremlin-says-absurd-suggest-russia-involved-baltic-sea-cable-damage-2024–11–20/.

139 Police of Finland, 'NBI launched a Criminal Investigation into Ruptured Undersea Cable in Baltic Sea', 20 November 2024, https://poliisi.fi/en/-/nbi-launched-a-criminal-investigation-into-ruptured-undersea-cable-in-baltic.

140 Christy Cooney, 'Sweden asks China to Co-operate over Severed Cables', BBC News, 29 November 2024, https://www.bbc.co.uk/news/articles/c748210k82wo.

141 Ministry of Foreign Affairs of the People's Republic of China, 'Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on November 29, 2024', 29 November 2024, https://www.fmprc.gov.cn/eng/xw/fyrbt/lxjzh/202411/t20241129_11535507.html.

142 Louise Rasmussen, 'China lets Sweden, Finland, Germany and Denmark board Ship in Cable Breach Case', Reuters, 19 December 2024, https://www.reuters.com/world/europe/swedish-police-go-board-yi-peng-3-vessel-invitation-china-2024–12–19/; Bojan Pancevski, 'China Lets European Investigators Board Ship Suspected of Sabotage After Weeks of Secret Talks, *Wall Street Journal*, 19 December 2024, https://www.wsj.com/world/china-lets-european-investigators-board-ship-suspected-of-sabotage-after-weeks-of-secret-talks-e68a2b75.

Initial reports suggested that the *Yi Peng 3* remained in Denmark's EEZ after the incident because it was detained there by Danish vessels.[143] However, it is far more likely that it remained at anchor because it was instructed to do so by the Chinese authorities. Whereas the People's Republic of China undoubtedly had the right, in fact the duty, to exercise both prescriptive and enforcement jurisdiction over the *Yi Peng 3* in its capacity as the flag state, it is not clear to what extent Denmark would have been entitled to do so as the coastal state.

Pursuant to Article 113 UNCLOS, every state must make it a punishable offence under its domestic law for a ship flying its flag or a person subject to its jurisdiction to break or 'injure' a submarine cable wilfully or through culpable negligence, or to engage in conduct calculated or likely to result in such breaking or injury. This means that the People's Republic of China was required to adopt domestic legislation to criminalize the breaking or injuring of submarine cables by ships flying its flag or by persons subject to its jurisdiction. However, Article 113 UNCLOS does not require or entitle coastal states to extend their domestic criminal law to ships not flying their flag. Moreover, since Article 113 UNCLOS only deals with prescriptive jurisdiction, the general rules of UNCLOS apply when it comes to enforcement. In the absence of specific enforcement authorities, coastal states cannot interdict foreign vessels in their EEZ suspected of breaking or injuring submarine cables without infringing on their freedom of navigation. Accordingly, the question arises whether Denmark was entitled to extend its criminal laws to the *Yi Peng 3* in the present case and, assuming it was, whether it could have enforced those laws.

As regards the exercise of prescriptive jurisdiction, the obligations imposed by Article 113 UNCLOS are aimed at flag states and states of nationality. However, nothing in that provision expressly prevents coastal states from extending their criminal laws to their own submarine cables pursuant to other well-established principles of jurisdiction, particularly the passive personality and the protective principle.[144] Evidently, states exercising their right to lay and operate submarine cables in accordance with UNCLOS have prescriptive jurisdiction over them. For example, all states are entitled to extend their domestic law on property ownership to their cables wherever they are located, including on the high seas.[145] In the absence of competing considerations, there is no reason why coastal states may not exercise prescriptive jurisdiction to make it a criminal offence for foreign vessels to break or injure their submarine cables in their EEZ.[146] However, in the present case, the cables in question were neither laid nor operated by Denmark and did not even

143 Bojan Pancevski, Sune Engel Rasmussen and Benoit Faucon, 'Chinese-Registered Ship Is Held in Baltic Sea Sabotage Investigation', 20 November 2024, https://www.wsj.com/world/europe/chinese-registered-ship-is-held-in-baltic-sea-sabotage-investigation-27929472.

144 Wolff Heintschel von Heinegg, 'Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law', in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, ed. Katharina Ziolkowski (Tallinn: NATO CCD COE, 2013), 291–318, 317.

145 This is implicit in Article 114, UNCLOS.

146 But see Xuexia Liao, 'Protection of Submarine Cables against Acts of Terrorism', *Ocean Yearbook*, Volume 33 (2019): 456–486, 461–465.

cross into its EEZ. Accordingly, it is unclear on what basis, if any, Denmark could have applied its criminal laws.

The exercise of enforcement jurisdiction also raises difficult questions.[147] Assuming that coastal states are entitled to extend their domestic criminal law to foreign vessels suspected of damaging their submarine cables in the EEZ, such authority would be meaningless unless it also implied a right to take measures necessary to enforce those rules. Although not without merit, this argument is open to objections. In essence, it takes the right of coastal states to exercise criminal jurisdiction on board foreign vessels, as recognized in Article 27 UNCLOS, and extends its applicability from the territorial sea into their EEZ. Whether doing so is compatible with UNCLOS remains an open question. In fact, states that have established protection zones around their submarine cables outside their territorial waters have not extended their criminal law to foreign nationals or foreign vessels in a comprehensive manner. For example, Australian legislation that makes it a criminal offence to damage Australian submarine cables applies outside territorial waters only to Australian nationals and vessels, but not to foreign nationals and vessels, unless the actions or omissions of the latter are done, touch upon, concern, arise out of, or are connected with the exploration of Australia's continental shelf, the exploitation of its resources or those of its EEZ, or the operations of artificial islands, installations or structures under Australia's jurisdiction.[148]

The Convention for the Protection of Submarine Telegraph Cables of 1884 does not assist either.[149] Assuming that the Convention applies to fibre optic communication cables at all,[150] it confers only very limited enforcement powers against foreign vessels suspected of damaging a submarine cable.[151] In any event, since neither of the cables allegedly damaged by the *Yi Peng 3* land on Danish territory or even cross the country's EEZ, Denmark could not have relied on the Convention in relation to the incident.[152] Even if it could have done so, the People's Republic of China is not a party to the Agreement,[153] and it is unlikely that its provisions on enforcement have passed into customary international law.[154]

Nor could Denmark have relied on the *Artic Sunrise* case to exercise its enforcement jurisdiction against the *Yi Peng 3*. As noted earlier, one of the principles recognized in that case

147 Robert Beckman, 'Protecting Submarine Cables from Intentional Damage – The Security Gap', in *Submarine Cables: The Handbook of Law and Policy*, ed. Douglas R. Burnett, Robert Beckman and Tara M. Davenport (Leiden: Brill, 2013), 281–297, 288–289.

148 Clause 44A, Schedule 3A, Telecommunications Act 1997.

149 Convention for the Protection of Submarine Telegraph Cables, 14 March 1884, 163 CTS 241.

150 The very limited state practice under the Convention does not relate to such cables. See United States Department of State, 'US and USSR Exchange of Notes on Damage to Submarine Cables', Department of State Bulletin, Vol. 40, Issue 1043, 20 April 1959, 555.

151 Article 10, Convention for the Protection of Submarine Telegraph Cables.

152 Article 2, Convention for the Protection of Submarine Telegraph Cables.

153 But see Efthymios Papastavridis, *The Interception of Vessels on the High Seas: Contemporary Challenges to the Legal Order of the Oceans* (Oxford: Hart, 2013), 34.

154 Ringbom and Lott, 'Sabotage of Critical Offshore Infrastructure', 176. Whereas some provisions of the Convention have been incorporated into UNCLOS, this is not the case for Article 10 of the Convention.

is that a coastal state is entitled to prevent interference with its sovereign rights for the exploration and exploitation of the non-living resources of its EEZ.[155] However, this principle would apply to submarine cables only if they were laid and operated by the coastal state to exploit the natural resources of its EEZ, but not if they are merely crossing its EEZ. Whether the reasoning of the *Artic Sunrise* case may be extended to such cables is unclear, and doing so may run into opposition.[156] Moreover, the principle only permits preventive or protective action in response to an unfolding incident; it would not have entitled Denmark to board and arrest the *Yi Peng 3* to enforce its domestic criminal laws after the event. For the same reasons, Denmark could not have justified boarding and arresting the vessel by invoking necessity as a circumstance precluding wrongfulness, as the ship posed no 'imminent' peril once it laid anchor.

Finally, Denmark could have invoked the rules relating to piracy. Contrary to what the *Arctic Sunrise* award suggests,[157] it is not an essential requirement that acts of piracy be directed against another ship.[158] Pursuant to Article 101 UNCLOS, the definition of piracy extends to illegal acts of violence committed for private ends by the crew of a private ship and directed against *property* in a place outside the jurisdiction of any state.[159] In principle, this brings violence directed against submarine cables within the scope of the definition. However, only deliberate acts are covered: accidental damage does not qualify. Nor do acts of violence committed on the instructions of a state or under its direction amount to piracy, since only acts committed for private ends fall within the definition.[160] Moreover, given that coastal states enjoy certain sovereign and jurisdictional rights in relation to the EEZ, it is not immediately clear whether that zone qualifies as 'a place outside the jurisdiction of any state'.[161] Although it would not have been implausible for Denmark to invoke the UNCLOS rules on piracy to arrest the *Yi Peng 3*, this would have been an unusual move. In the absence of compelling reasons

155 *Arctic Sunrise*, para. 324.

156 International Law Association, Committee on Submarine Cables and Pipelines under International Law, 'Third Interim Report', 2024, 18–19.

157 *Arctic Sunrise*, para. 238.

158 See also Douglas Guilfoyle, Tamsin Phillipa Paige and Rob McLaughlin, 'The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables', *International and Comparative Law Quarterly*, Volume 71 (2022): 657–696, 671.

159 Article 101(a)(ii), UNCLOS.

160 See also Alexander Lott, 'The Baltic Sea Cable-Cuts and Ship Interdiction: The C-Lion1 Incident', Articles of War, 26 November 2024, https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/.

161 The better view is that it does. Although by referring to a 'place outside the jurisdiction of any State', the International Law Commission 'had chiefly in mind acts committed by a ship or aircraft on an island constituting *terra nullius* or on the shores of an unoccupied territory', the underlying principle of its definition was that piracy cannot be committed inside the territory or territorial waters of a state. Accordingly, this does exclude an EEZ. See Commentaries to the Articles Concerning the Law of the Sea, in International Law Commission, Report of the International Law Commission on the Work of its Eighth Session, 23 April–4 July 1956, Official Records of the General Assembly, Eleventh Session, Supplement No. 9 (A/3159), Article 39 and its commentary.

suggesting that the ship's actions fell within the definition of piracy, China would most likely have objected strongly to such an arrest as a violation of its exclusive flag-state jurisdiction.

4.3 The use of force

Efforts to counter maritime hybrid threats must also take into account the rules governing the use of force set out in the United Nations Charter. First, all states are bound by the obligation not to use force in their international relations.[162] This means that law enforcement and protective measures taken against hybrid threat activities must be carefully distinguished from unlawful uses of force. Second, should hybrid threat activities amount to an armed attack, they give rise to the right of individual and collective self-defence, entitling states to respond with necessary and proportionate counterforce.[163] The question therefore arises as to the circumstances under which harmful acts directed against maritime infrastructure reach the level of an armed attack.

All states are prohibited from using force in their international relations. This principle is set out in Article 2(4) of the United Nations Charter, but also forms part of customary international law and is widely recognized as one of the foundational principles of the modern international legal order.[164] The term 'force' refers primarily to armed force. The prohibition therefore covers classic acts of warfare, such as invasion or bombardment,[165] but does not apply to mere economic pressure or other forms of coercion. The prohibition is not limited to the use of conventional military means. As the International Court of Justice has confirmed, the rule applies regardless of the weapon used.[166] There is some debate as to whether forcible measures must attain a minimum degree of intensity to fall within the scope of Article 2(4) of the Charter.[167] State practice suggests that the intensity of the violence is a relevant factor in determining whether or not it amounts to a use of force within the meaning of the Charter, but it does not clearly establish the existence of a minimum intensity threshold.[168]

The concept of force is not rigidly defined. While this flexibility contributes to the effectiveness of Article 2(4) of the Charter, it also makes it more difficult to distinguish measures of maritime law enforcement from prohibited uses of force. In the exercise of their nation's enforcement jurisdiction, government vessels may compel other ships to submit to their authority, including by resorting to violence or the threat of violence.[169] Such activities may easily be mistaken for a prohibited use of

162 Article 2(4), United Nations Charter.
163 Article 51, United Nations Charter.
164 *Nicaragua (Merits)*, para. 190.
165 See Article 3, United Nations General Assembly, Definition of Aggression, UN Doc. A/RES/3314(XXIX), 14 December 1974.
166 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) (1996) ICJ Rep. 226, para. 39.
167 Terry D. Gill and Kinga Tibori-Szabó, *The Use of Force and the International Legal System* (Cambridge: Cambridge University Press, 2023), 63–64.
168 See Tom Ruys, 'The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of Force Excluded from UN Charter 2(4)?', *American Journal of International Law*, Volume 108 (2014): 159–210.
169 E.g. *Fisheries Jurisdiction Case (Spain v. Canada)* (Judgment) (1998) ICJ Rep. 432, paras 78–84. See Matteo Tondini, 'The Use of Force in the Course of Maritime Law Enforcement Operations', *Journal on the Use of Force and International Law*, Volume 4 (2017): 253–272.

force,[170] given that Article 2(4) applies irrespective of the means employed, does not require any particular level of intensity, and prohibits not only the actual use of force, but also the threat of violence. However, the two concepts – maritime law enforcement and the use of force – are normatively distinct.[171]

A number of factors should be considered when distinguishing between the exercise of law enforcement powers and the use of force. First, forcible action not involving conventional military means may still qualify as force within the meaning of Article 2(4) if it is capable of bringing about violent effects. Second, even in the absence of a minimum intensity threshold, the gravity of the violence is relevant. The more significant its scale and effects, the more likely it is that it amounts to a use of force.[172] Third, violence employed in the exercise of recognized law enforcement powers is unlikely to constitute a use of force, even where it is based on a good-faith mistake of fact.[173] Fourth, taking forcible measures against vessels benefitting from sovereign immunity is likely to amount to a use of force.[174] Fifth, where violence is threatened or used against private vessels in disputed waters, the incident is more likely to be international in character and therefore to fall within the scope of Article 2(4) of the Charter.[175] Finally, consideration must be given to the overall context and conduct of the parties, including whether a vessel purporting to engage in law enforcement is in fact taking measures consistent with the exercise of such powers.[176]

The key point is that states taking operational action against suspicious foreign vessels – by stretching existing legal authorities, applying them in novel circumstances, or extending their scope beyond established precedents – expose themselves not only to accusations of interfering with the freedoms of the flag state, but also to allegations of using force in contravention of Article 2(4) of the Charter where their action involves violence or the threat of violence.[177] This risk also arises should states rely on the *Arctic Sunrise* principles to take preventive or

170 See also Patricia Jimenez Kwast, 'Maritime Law Enforcement and the Use of Force: Reflections on the Categorisation of Forcible Action at Sea in the Light of the Guyana/Suriname Award', *Journal of Conflict and Security Law*, Volume 13 (2008): 49–91.

171 This is implicit in UNCLOS, which confers various law enforcement powers onto states, but requires them to refrain from any threat or use of force in Article 301, UNCLOS.

172 Christian Henderson, *The Use of Force and International Law* (2nd edn, Cambridge: Cambridge University Press, 2024), 130.

173 Cf. *The 'Enrica Lexie' Incident (Italy v. India)* (2020) Award, 21 May 2020 (Arbitral Tribunal instituted under Annex VII to UNCLOS), para. 1076–1077.

174 *The 'ARA Libertad' Case (Argentina v. Ghana), Provisional Measures* (2012) Order, 15 December 2012 (International Tribunal for the Law of the Sea), para. 97.

175 *Guyana v. Suriname* (2007) Award, 17 September 2007 (Arbitral Tribunal constituted under Article 287 and Annex II to UNCLOS), paras 425–447 and 484.

176 Cf. *The M/V 'Saiga' (No. 2) Case (Saint Vincent and the Grenadines v. Guinea)* (1999) Judgment, 1 July 1999 (International Tribunal for the Law of the Sea), paras 153–159. See also Aurel Sari, 'Maritime Incidents in the South China Sea: Measures of Law Enforcement or Use of Force?', *International Law Studies*, Volume 103 (2024): 463–511, 499–500.

177 Cf. Douglas Guilfoyle, *Shipping Interdiction and the Law of the Sea* (Cambridge: Cambridge University Press, 2009), 277.

protective action against vessels interfering with the exercise of their sovereign rights or posing a terrorist threat, as the dividing line between those principles and the use of force remains unclear.

The rules governing the use of force may also be invoked when malign actors use violence against critical maritime infrastructure, such as severing submarine cables. In addition to the factors just discussed, two points require careful scrutiny to determine whether such violence amounts to a use of force prohibited by Article 2(4) of the Charter. First, the prohibition applies only at the level of 'international relations'. Unless the violence occurs in that context, which usually means between at least two states, it will not be covered by Article 2(4). Accordingly, if forcible action was taken by a non-state actor and its actions cannot be attributed to a state, the prohibition will not be engaged. Similarly, where forcible action was directed against privately owned infrastructure located outside territorial waters, it is unlikely to have occurred at the level of 'international relations'. Second, since physical harm caused by an accident falls outside the scope of Article 2(4), it is necessary to establish whether the forcible action was taken deliberately or not.

Although the answers to these two questions are important, the fact that force within the meaning of the United Nations Charter was used against a state's maritime infrastructure does not entitle that state to respond with counterforce in the exercise of the right of self-defence, unless the initial use of force rises to the level of an armed attack. According to the International Court of Justice, an armed attack as understood within the meaning of Article 51 of the United Nations Charter refers to 'the most grave forms of the use of force'.[178] The Court has held that an armed attack must be more severe than a 'mere frontier incident' in terms of its scale and effects,[179] but this does not exclude the possibility that the mining of a single military vessel might suffice to cross that threshold.[180] Several questions arise when applying these principles to attacks against maritime infrastructure.

It is not self-evident that the severing of a submarine cable or pipeline with an anchor can be equated, in terms of its gravity, to the mining of a military vessel. The economic and societal impact of a severed submarine communication cable might be significant, but the scale and impact of the damage suffered by the cable itself will most likely pale in comparison to the damage that a naval mine might inflict upon a warship. Dissatisfied with the kinetic focus of the law, some states have advocated a different approach in the context of cyberspace. France, for example, has taken the view that a cyber operation causing significant economic damage may amount to an armed attack, even where it does not involve the loss of life or physical destruction.[181] Singapore has taken a similar position, declaring that in cer-

178 *Nicaragua (Merits)*, para. 191. This point is well-established: e.g. Eritrea-Ethiopia Claims Commission, 'Partial Award: *Jus Ad Bellum* – Ethiopia's Claims 1–8' (XXVI Reports of International Arbitral Awards, 2009), at para. 11.

179 *Nicaragua (Merits)*, para. 195.

180 *Case Concerning Oil Platforms (Iran v. USA)*, (2003) ICJ Rep. 161, para. 72.

181 Ministère des Armés, 'Droit international appliqué aux opérations dans le cyberespace' [Ministry of Defence, International law applied to operations in cyberspace] (2019), 9.

tain circumstances, malicious cyber activities may qualify as an armed attack even without causing injury or physical damage, for example where they cause a sustained and long-term outage of Singapore's critical infrastructure.[182] There is no reason why this approach could not be extended to critical maritime infrastructure to suggest that attacks causing significant economic damage may qualify as an armed attack even if they cause only minor kinetic harm. However, this is an unorthodox position that is unlikely to attract widespread support among states, at least for now.

States on the receiving end of hybrid threat attacks are more likely to resort to the accumulation of events doctrine, whereby the effects of a series of incidents, which remain below the threshold of an armed attack when seen in isolation, are considered cumulatively, thereby potentially passing the gravity threshold.[183] However, applying the accumulation of events doctrine to repeated attacks against maritime infrastructure will only engage the right of self-defence if those attacks can be attributed to the same actor. This may prove difficult. Moreover, in the case of assets that do not belong to a single state, but connect several countries, principally submarine cables and pipelines, it is not immediately clear which of the states concerned should be considered the victim of the potential armed attack and thus entitled to invoke the right of self-defence.[184]

A final point to bear in mind is that even if the right of self-defence were to be invoked in the case of an armed attack against critical maritime infrastructure, any use of force in self-defence must comply with the requirements of necessity and proportionality.[185] This is not just a technical requirement, but raises a broader question about the strategic utility of counterforce in responding to hybrid threat activities: where a state has suffered a small-scale armed attack and now has a legal right to respond by using force, doing so against a credible and determined adversary may pose a significant escalation risk that effectively rules out even the limited use of counterforce as a viable response option.

182 United Nations General Assembly, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law applies to the Use of Information and Communications Technologies by States submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266', UN Doc. A /76/136, 84.

183 In relation to the use of force, see Council of the European Union, 'Declaration on a Common Understanding of International Law in Cyberspace', Council doc. 15833/24, 18 November 2024, 6.

184 See also Danae Azaria and Geir Ulfstein, 'Are Sabotage of Submarine Pipelines an 'Armed Attack' Triggering a Right to Self-defence?', EJIL:Talk, 18 October 2022, https://www.ejiltalk.org/are-sabotage-of-submarine-pipelines-an-armed-attack-triggering-a-right-to-self-defence/.

185 See Chris O'Meara, *Necessity and Proportionality and the Right of Self-Defence in International Law* (Oxford: Oxford University Press, 2021).

5. Conclusions

The maritime domain plays a central role in global trade, security and communications. Maritime infrastructure will therefore remain a prime target for hybrid threats. Recent incidents in the Baltic Sea and the North Sea clearly underscore the vulnerabilities in this area. The existing legal regimes, particularly the law of the sea, serve as a framework for addressing these vulnerabilities, but as this report has shown, significant gaps remain. While the law confers extensive authorities on states to maintain situational awareness in the maritime environment, their powers to take appropriate operational action to counter hybrid threat activities are less comprehensive. Various gaps exist, especially with regard to the protection of submarine communication cables.

Protecting critical maritime infrastructure from hybrid threats requires a proactive and multi-faceted approach. The availability of robust legal authorities and close cooperation across what is a fragmented jurisdictional landscape are key. In this context, EU member states and NATO allies may consider a number of steps.

First, as part of a legal resilience approach, they should take stock of their domestic laws to determine whether they have made full use of their right to exercise prescriptive jurisdiction under UNCLOS. Specifically, they should identify any gaps in the application of their domestic criminal and civil laws that hybrid threat actors may be able to exploit.

Second, they should explore the kind of legal structures and processes that are available to enable close collaboration between different national authorities, for instance in the exercise of enforcement powers, in situations where hybrid threat activities take place in the territorial waters or EEZ of one coastal state, but the perpetrator is present in the waters or EEZ of another state, as in the case of the *Yi Peng 3*. This may require harmonizing domestic legislation to allow international cooperation across jurisdictional boundaries.

Third, they should consider the extent to which dynamic or innovative interpretations of existing rules, such as the duty to cooperate in the suppression of piracy and the rules on environmental protection, may address some of the gaps and other shortcomings in the regulatory framework, principally the law of the sea. In this context, they should also consider the role that circumstances precluding wrongfulness, in particular necessity,[186] and the adoption of countermeasures may play.[187] Adopting a common position on these matters and coordinating with like-minded nations will be critical to the success of taking a more dynamic approach.

Fourth, they should collaborate to further reinforce mechanisms for information sharing and for the individual and collective attribution of hybrid threats.

Finally, they should make a concerted diplomatic effort to strengthen broader international cooperation for protecting critical maritime infrastructure, including by encouraging all states to adhere to their obligations under Article 113 UNCLOS and exploring options for creating new international rules for the protection of submarine cables and pipelines.[188]

186 Article 25, Draft Articles on the Responsibility. See International Law Association, Third Interim Report, 20.

187 See Raul (Pete) Pedrozo, 'Safeguarding Submarine Cables and Pipelines in Times of Peace and War', *International Law Studies*, Volume 106 (2025): 45–65, 62–65.

188 Cf. Thea Coventry, 'What should States do to Combat the Sabotage of Submarine Cables and Pipelines beneath the High Seas/EEZs?', EJIL:Talk, 13 December 2024, https://www.ejiltalk.org/what-should-states-do-to-combat-the-sabotage-of-submarine-cables-and-pipelines-beneath-the-high-seas-eezs/.

Bibliography

Ahlander, Johan. 'Danish Military says It's Staying close to Chinese Ship after Data Cable Breaches', Reuters, 20 November 2024. https://www.reuters.com/world/europe/kremlin-says-absurd-suggest-russia-involved-baltic-sea-cable-damage-2024–11–20/.

Ashford, Warwick. 'NotPetya attack cost up to $300m, says Maersk', Computer Weekly, 17 August 2017. https://www.computerweekly.com/news/450424559/NotPetya-attack-cost-up-to-300m-says-Maersk.

Azaria, Danae and Ulfstein, Geir. 'Are Sabotage of Submarine Pipelines an 'Armed Attack' Triggering a Right to Self-defence?', EJIL:Talk, 18 October 2022. https://www.ejiltalk.org/are-sabotage-of-submarine-pipelines-an-armed-attack-triggering-a-right-to-self-defence/.

Baltic Sentinel. 'Swift Action by Finnish Authorities Prevented Cable-Sabotaging Tanker from Damaging Balticconnector Pipeline', 28 December 2024. https://balticsentinel.eu/8162178/swift-action-by-finnish-authorities-prevented-cable-sabotaging-tanker-from-damaging-balticconnector-pipeline.

Barnes, Richard. 'Article 27'. In *United Nations Convention on the Law of the Sea: A Commentary*, edited by A. Proelss. München: C. H. Beck, 2017, 229–237.

Beckman, Robert. 'Protecting Submarine Cables from Intentional Damage – The Security Gap'. In *Submarine Cables: The Handbook of Law and Policy*, edited by D. R. Burnett, R. Beckman and T. M. Davenport. Leiden: Brill, 2013, 281–297.

Braw, Elisabeth. 'The Baltic Sea's Bad Actors', Foreign Policy, 4 December 2024. https://foreignpolicy.com/2024/12/04/russia-china-baltic-sea-nato-subsea-cables-ais-spoofing/.

Bueger, Christian. 'Maritime Security in the Age of Infrastructure'. *ASCOMARE Yearbook on the Law of the Sea*, Volume 3, (2023): 73–88.

Bueger, Christian and Liebetrau, Tobias. 'Critical Maritime Infrastructure Protection: What's the Trouble?'. *Marine Policy*, Volume 155, (2023): 1–8.

Burnett, Douglas R. 'Submarine Cable Security and International Law'. *International Law Studies*, Volume 97, (2021): 1659–1682.

Cheetham, Joshua and Walker, Amy. 'Ship Carrying Explosive Fertiliser heads to UK Waters', BBC, 26 September 2024. https://www.bbc.co.uk/news/articles/c62g95721leo.

Cooney, Christy. 'Sweden asks China to Co-operate over Severed Cables', BBC News, 29 November 2024. https://www.bbc.co.uk/news/articles/c748210k82wo.

Coventry, Thea. 'What should States do to Combat the Sabotage of Submarine Cables and Pipelines beneath the High Seas/EEZs?', EJIL:Talk, 13 December 2024. https://www.ejiltalk.org/what-should-states-do-to-combat-the-sabotage-of-submarine-cables-and-pipelines-beneath-the-high-seas-eezs/.

Crawford, James. *State Responsibility: The General Part*. Cambridge: Cambridge University Press, 2013.

Doğan, Diren and Çetikli, Deniz. *Maritime Critical Infrastructure Protection (MCIP) in a Changing Security Environment*. NATO Maritime Security Centre of Excellence, 2023.

Giannoulis (ed), Georgios. *Handbook on Maritime Hybrid Threats: 15 Scenarios and Legal Scans*. Hybrid CoE Paper 16. The European Centre of Excellence for Countering Hybrid Threats, 2023.

Gill, Terry D. and Tibori-Szabó, Kinga. *The Use of Force and the International Legal System*. Cambridge: Cambridge University Press, 2023.

Guilfoyle, Douglas. *Shipping Interdiction and the Law of the Sea*. Cambridge: Cambridge University Press, 2009.

Guilfoyle, Douglas, Paige, Tamsin Phillipa and McLaughlin, Rob. 'The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables'. *International and Comparative Law Quarterly*, Volume 71, (2022): 657–696.

Harrison, James. 'Safeguards against Excessive Enforcement Measures in the Exclusive Economic Zone—Law and Practice'. In *Jurisdiction over Ships: Post-UNCLOS Developments in the Law of the Sea*, edited by H. Ringbom. Leiden: Brill, 2015, 217–248.

Hayashi, Moritaka. 'Military and Intelligence Gathering Activities in the EEZ: Definition of Key Terms'. *Marine Policy*, Volume 29, (2005): 123–137.

Hebbar, Anish Arvind, Schröder-Hinrichs, Jens-Uwe and Yildiz, Serdar. 'Vessel Traffic Management in the Era of Maritime Autonomous Surface Ships and Digitalization: Experiences in European Waters'. In *Area-Based Management of Shipping: Canadian and Comparative Perspectives*, edited by A. Chircop, F. Goerlandt, R. Pelot and C. Aporta. Cham: Springer, 2024, 185–205.

Heintschel von Heinegg, Wolff. 'Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law'. In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by K. Ziolkowski. Tallinn: NATO CCD COE, 2013, 291–318.

Helsinki Times. 'Finnish Court Denies Release of Tanker in Undersea Cables Investigation', 3 January 2025. https://www.helsinkitimes.fi/finland/finland-news/domestic/25932-finnish-court-denies-release-of-tanker-in-undersea-cables-investigation.html.

Henderson, Christian. *The Use of Force and International Law*. Cambridge: Cambridge University Press, 2024, 2nd edn.

Hillman, Jonathan E. *Securing the Subsea Network: A Primer for Policymakers*. Center for Strategic and International Studies 2021.

Kajitani, Yoshio, Chang, Stephanie E. and Tatano, Hirokazu. 'Economic Impacts of the 2011 Tohoku-Oki Earthquake and Tsunami'. *Earthquake Spectra*, Volume 29, (2013): 457–478.

Kauranen, Anne and Adomaitis, Nerijus 'Recent Suspected Underwater Sabotage Incidents in the Baltic Sea', Reuters, 3 December 2024. https://www.reuters.com/world/europe/recent-suspected-underwater-sabotage-incidents-baltic-sea-2024-12-03/.

Kaushal, Sidharth. 'Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure', Royal United Services Institute, 25 May 2023. https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure.

Kaye, Stuart B. 'Freedom of Navigation, Surveillance and Security: Legal Issues Surrounding the Collection of Intelligence from Beyond the Littoral'. *Australian Yearbook of International Law*, Volume (2005): 93–105.

Khan, Daniel-Erasmus. 'Article 33'. In *United Nations Convention on the Law of the Sea: A Commentary*, edited by A. Proelss. München: C. H. Beck, 2017, 254–271.

King, Jordan and Feng, John. 'Chinese Ship May Have Tried to Sabotage Undersea Cables Before', Newsweek, 18 December 2024. https://www.newsweek.com/chinese-ship-yi-peng-3-undersea-cables-damage-2002637.

Klein, Natalie. *Maritime Security and the Law of the Sea*. Oxford: Oxford University Press, 2011.
Kraska, James. 'Intelligence Collection and the International Law of the Sea'. *International Law Studies*, Volume 99, (2022): 602–637.

Kwast, Patricia Jimenez. 'Maritime Law Enforcement and the Use of Force: Reflections on the Categorisation of Forcible Action at Sea in the Light of the Guyana/Suriname Award'. *Journal of Conflict and Security Law*, Volume 13, (2008): 49–91.

Lehr, Peter. *A Modern History of Maritime Terrorism: From the Fenian Ram to Explosive-Laden Drone Boats*. Cheltenham: Edward Elgar, 2023.

Letts, David. 'The Maritime Domain'. In *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, edited by M. Regan and A. Sari. New York: Oxford University Press, 2024, 251–270.

Liao, Xuexia. 'Protection of Submarine Cables against Acts of Terrorism'. *Ocean Yearbook*, Volume 33, (2019): 456–486.

Lott, Alexander. 'The Baltic Sea Cable-Cuts and Ship Interdiction: The C-Lion1 Incident', Articles of War, 26 November 2024. https://lieber.westpoint.edu/baltic-sea-cable-cuts-ship-interdiction-c-lion1-incident/.

Lott, Alexander. *Hybrid Threats and the Law of the Sea: Use of Force and Discriminatory Navigational Restrictions in Straits*. Leiden: Brill, 2022.

Lott, Alexander (ed.) *Maritime Security Law in Hybrid Warfare* (Brill 2024).

Miller, Greg. 'Billions in Damage Claims Pile Up in Response to Baltimore Bridge Disaster', Lloyd's List, 24 September 2024. https://www.lloydslist.com/LL1150755/Billions-in-damage-claims-pile-up-in-response-to-Baltimore-bridge-disaster.

Ministère des Armés. *Droit international appliqué aux opérations dans le cyberespace*. 2019.

Mossop, Joanna. 'Protests against Oil Exploration at Sea: Lessons from the Arctic Sunrise Arbitration'. *International Journal of Marine and Coastal Law*, Volume 31, (2016): 60–87.

Notteboom, Theo, Haralambides, Hercules and Cullinane, Kevin. 'The Red Sea Crisis: Ramifications for Vessel Operations, Shipping Networks, and Maritime Supply Chains'. *Maritime Economics and Logistics*, Volume 26, (2024): 1–20.

O'Meara, Chris. *Necessity and Proportionality and the Right of Self-Defence in International Law*. Oxford: Oxford University Press, 2021.

Østhagen, Andreas. *The Arctic after Russia's Invasion of Ukraine: The Increased Risk of Conflict and Hybrid Threats*. Hybrid CoE Paper 18. The European Centre of Excellence for Countering Hybrid Threats, 2023.

Paddeu, Federica. 'Clarifying the Concept of Circumstances Precluding Wrongfulness (Justifications) in International Law'. In *Exceptions in International Law*, edited by L. Bartels and F. Paddeu. Oxford University Press, 2020, 203–224.

Pancevski, Bojan. 'China Lets European Investigators Board Ship Suspected of Sabotage After Weeks of Secret Talks', Wall Street Journal, 19 December 2024. https://www.wsj.com/world/china-lets-european-investigators-board-ship-suspected-of-sabotage-after-weeks-of-secret-talks-e68a2b75.

Pancevski, Bojan, Rasmussen, Sune Engel and Faucon, Benoit. 'Chinese-Registered Ship Is Held in Baltic Sea Sabotage Investigation', Wall Street Journal, 20 November 2024. https://www.wsj.com/world/europe/chinese-registered-ship-is-held-in-baltic-sea-sabotage-investigation-27929472.

Papastavridis, Efthymios. *The Interception of Vessels on the High Seas: Contemporary Challenges to the Legal Order of the Oceans*. Oxford: Hart, 2013.

Pedrozo, Raul (Pete). 'Safeguarding Submarine Cables and Pipelines in Times of Peace and War'. *International Law Studies*, Volume 106, (2025): 45–65.

Precey, Matt. 'How an Explosion-risk Ship ended up in Norfolk', BBC, 22 November 2024. https://www.bbc.co.uk/news/articles/c2062g4dzwro.

Rasmussen, Louise. 'China lets Sweden, Finland, Germany and Denmark board Ship in Cable Breach Case', Reuters, 19 December 2024. https://www.reuters.com/world/europe/swedish-police-go-board-yi-peng-3-vessel-invitation-china-2024–12–19/.

Redgwell, Catherine. 'Property Law Sources and Analogies in International Law'. In *Property and the Law in Energy and Natural Resources*, edited by A. McHarg, B. Barton, A. Bradbrook and L. Godden. Oxford University Press, 2010, 100–112.

Ringbom, Henrik and Lott, Alexander. 'Sabotage of Critical Offshore Infrastructure: a Case Study of the Balticconnector Incident'. In *Maritime Security Law in Hybrid Warfare*, edited by A. Lott. Leiden: Brill, 2024, 155–194.

Rodriguez-Diaz, Emilio, Alcaide, J. I. and Garcia-Llave, R. 'Challenges and Security Risks in the Red Sea: Impact of Houthi Attacks on Maritime Traffic'. *Journal of Marine Science and Engineering*, Volume 12, (2024): 1–18.

Roggenkamp, Martha M. 'Petroleum Pipelines in the North Sea: Questions of Jurisdiction and Practical Solutions'. *Journal of Energy and Natural Resources Law*, Volume 16, (1998): 92–109.
Ruys, Tom. 'The Meaning of 'Force' and the Boundaries of the Jus Ad Bellum: Are 'Minimal' Uses of

Force Excluded from UN Charter 2(4)?'. *American Journal of International Law*, Volume 108, (2014): 159–210.

Sari, Aurel. *Hybrid Threats and the Law: Building Legal Resilience*. Hybrid CoE Research Report 3. The European Centre of Excellence for Countering Hybrid Threats, 2021.

Sari, Aurel. 'Maritime Incidents in the South China Sea: Measures of Law Enforcement or Use of Force?'. *International Law Studies*, Volume 103, (2024): 463–511.

Schaller, Christian. 'Russia's Mapping of Critical Infrastructure in the North and Baltic Seas: International Law as an Impediment to Countering the Threat of Strategic Sabotage?'. *Nordic Journal of International Law*, Volume 93, (2024): 202–236.

Schwirtz, Michael, Xiao, Muyi and Mellen, Riley. 'EU Vessels Surround Anchored Chinese Ship After Baltic Sea Cables are Severed', The New York Times, 27 November 2024. https://www.nytimes.com/2024/11/27/world/europe/baltic-sea-cables-chinese-ship.html.

Senarak, Chalermpong. 'Port Cyberattacks from 2011 to 2023: A Literature Review and Discussion of Selected Cases'. *Maritime Economics and Logistics*, Volume 26, (2024): 105–130.

Shearer, I. A. 'Problems of Jurisdiction and Law Enforcement Against Delinquent Vessels'. *International and Comparative Law Quarterly*, Volume 35, (1986): 320–343.

Smith, Hance D., de Vivero, Juan Luis Suárez and Agardy, Tundi S. 'The World Ocean and The Human Past and Present'. In *Routledge Handbook of Ocean Resources and Management*, edited by H. D. Smith, J. L. S. de Vivero and T. S. Agardy. London: Routledge, 2015, 5–13.

Soldi, G., Gaglione, D., Raponi, S., Forti, N., d'Afflisio, E., Kowalski, P., Millefiori, L. M., Zissis, D., Braca, P., Willett, P., Maguer, A., Carniel, S., Sembenini, G. and Warner, C. 'Monitoring of Critical Undersea Infrastructures: The Nord Stream and Other Recent Case Studies'. *IEEE Aerospace and Electronic Systems Magazine*, Volume 38, (2023): 4–24.

Stensrud, Cecilie Juul and Østhagen, Andreas. 'Hybrid Warfare at Sea? Russia, Svalbard and the Arctic'. *Scandinavian Journal of Military Studies*, Volume 7, (2024): 111–130.

Tanaka, Yoshifumi. *The International Law of the Sea*. Cambridge: Cambridge University Press, 2012.

Tondini, Matteo. 'The Use of Force in the Course of Maritime Law Enforcement Operations'. *Journal on the Use of Force and International Law*, Volume 4, (2017): 253–272.

Tran, Nguyen Khoi, Haralambides, Hercules, Notteboom, Theo and Cullinane, Kevin. 'The Costs of Maritime Supply Chain Disruptions: The Case of the Suez Canal Blockage by the 'Ever Given' Megaship'. *International Journal of Production Economics*, Volume 279, (2025): 1–16.

U.S. Embassy Maldives, 'Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World', 29 January 2025. https://mv.usembassy.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/.

Author

Dr Aurel Sari is a Professor of Public International Law at the University of Exeter (United Kingdom). His work focuses primarily on international conflict and security law and the law relating to military operations. He has published widely on the law of armed conflict, status of forces agreements, peace support operations, international human rights law, and the legal framework of European security and defence policy. He has also spoken and written extensively on the legal aspects of hybrid warfare, including at the invitation of the Council of Europe, the European Commission, NATO and various government departments.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats