CHINA STRATEGIC RISKS INSTITUTE

DSET

Research Institute for **Democracy**, **Society**, and **Emerging Technology**

Testing the waters: Securing the UK's undersea cables against grey-zone threats

Andrew Yeh

June 2025

About the China Strategic Risks Institute

The China Strategic Risks Institute (CSRI) is a global policy think tank providing in-depth analysis of the risks and opportunities posed by the rise of the People's Republic of China. We aim for our research to be accessible to the general public, with recommendations for policymakers, international businesses and NGOs.

www.csri.global

About the Research Institute for Democracy, Society and Emerging Technology

DSET stands at the forefront of Taiwan's democratic values, weaving these principles into the very fabric of our policy research. As emerging technologies reshape the global landscape, they bring a mix of opportunities and challenges that touch every aspect of political and social spheres. We are committed to crafting governance frameworks for technology that not only protect security but also uphold freedom and sustainability. Our mission is to steer through this new terrain, ensuring that innovation serves democracy, and freedom remains at the heart of technological advancement.

https://dset.tw/

Research Institute for **Democracy**, **Society**, and **Emerging Technology**

Acknowledgements

The author would like to extend his gratitude to all the researchers and experts who contributed to this report. In particular, the author would like to thank the Energy Security and Climate Resilience and National Security teams at the Research Institute for Democracy, Society and Emerging Technology (DSET) for their contributions to research, analysis and review; Owen Au for major contributions to case study collection and analysis; Athena Tong, Visiting Researcher at the University of Tokyo, and Tau Yang for their additional research contribution, analysis and editing; and Kenny Huang, Jade McGlynn, Wenchi Yu and many other experts who gave their valuable insights and feedback.

Table of Contents

Key Point Summary

- Undersea cables underpin economic security and global prosperity in the digital age, carrying 99% of intercontinental data traffic. Undersea cables are vital for both civilian and defence infrastructure, including future AI-powered technologies.

- A series of suspicious breakages in the Baltic Sea and Taiwan Strait indicate that China and Russia may be using undersea sabotage as part of broader grey-zone operations against their adversaries – including NATO and its member states.

- This paper examines 12 suspected undersea cable sabotage cases from January 2021 to April 2025. Of the 10 with identified vessels, 8 are linked to China or Russia by flag or ownership.

- The involvement of Chinese vessels in cable breakages in Europe, and Russian vessels near Taiwan, suggests plausible China-Russia coordination amid deepening ties in both the Euro-Atlantic and Indo-Pacific.

- As a key hub in Euro-Atlantic cable infrastructure, the UK is a likely target for future Russian and Chinese grey-zone operations – posing a new and complex challenge for its maritime defence and surveillance systems.

- The UK must be clear-eyed and proactive in addressing grey-zone threats to undersea infrastructure. Recommendations include:

    - **Enhancing monitoring and surveillance:** The UK should use NATO mechanisms to regularly share best practice and intelligence on undersea cable threats, including Russia and China's shadow fleets, and extend cooperation to experienced partners like Taiwan and Japan.

    - **Strengthening mechanisms for accountability:** International law on undersea cables is outdated and insufficient. The UK should work with partners to strengthen accountability powers through utilising Port State Controls and publishing vessel blacklists. It must also tighten domestic laws and establish protocols for rapid pursuit, interdiction, and detention of suspect vessels.

    - **Improving redundancy, repair and resilience:** The UK government should work with private operators to ensure guaranteed access to cable repair vessels capabilities during crises or national emergencies, as well as strategic stockpiling of cable repair parts.

Introduction: Why do undersea cables matter?

Undersea cables underpin economic security and global prosperity in the digital age. The importance of undersea cables to internet connectivity is difficult to understate. Up to 99% of intercontinental data transmission takes place through submarine cable systems. While recent advances in satellite-based internet systems such as Starlink have grabbed headlines, submarine cables are still far faster, cheaper and more reliable.

Without undersea cables, much of the economy – from international banking and cloud computing to virtual communications and global logistics – would cease to function. As governments and private companies increasingly look to adopt AI-driven technologies, undersea cables will only become even more critical. Developing and operationalising AI requires vast amounts of data transfer, all of which will be reliant on undersea cables for transport between servers internationally. For this reason, many of the world's most ambitious undersea cable projects are being funded by technology companies aiming to provide the infrastructure for future AI-services.[1]

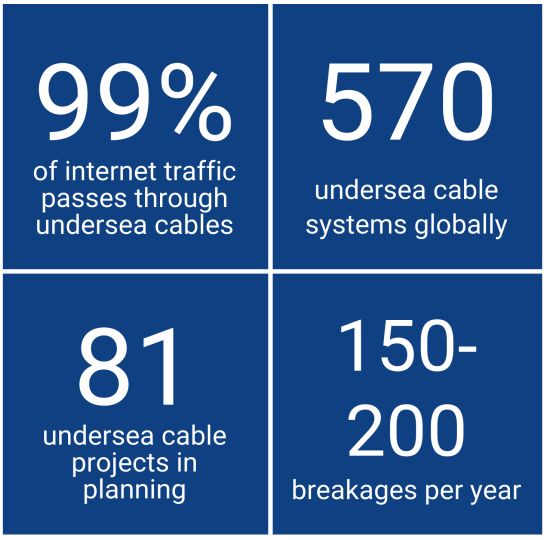


Figure: Importance of undersea cables globally[2]

Most undersea cables are dual-use in nature, supporting diplomatic, military and intelligence communications, as well as commercial uses. Notably, the growing reliance on 5G telecommunications for intelligence-sharing, command and coordination between NATO forces, means that damage to undersea cables could significantly deplete NATO's operational readiness.[3] While satellite-based communication systems can play an important role as back-up systems for some elements of critical communications infrastructure, the large amounts of data transfer that commercial, personal and non-critical government communications currently rely on will continue to be dependent on undersea cables.

Despite their critical importance, undersea cables have proven to be highly vulnerable to disruption. While the vast majority of breakages are thought to be accidental or due to natural factors, a series of breakages caused by vessels acting suspiciously in contested

[1] McMahon, 'Meta Plans Globe-Spanning Sub-Sea Internet Cable'.
[2] Park, 'The Deep-Sea "emergency Service" That Keeps the Internet Running'.
[3] Wall and Morcos, 'Invisible and Vital: Undersea Cables and Transatlantic Security'.

geopolitical hotspots has raised awareness that undersea cables are also highly vulnerable to sabotage by malicious actors.

The first section of this paper analyses the role of undersea cable sabotage in China and Russia's 'grey-zone' warfare strategies. Our analysis gathers evidence from 12 incidents of suspected sabotage against undersea infrastructure globally between 2021 and April 2025, with vessels directly linked to China and Russia in 8 out of the 10 cases in which a suspect vessel has been identified. While direct proof of intent is extremely difficult to prove in each instance, **undersea cable sabotage is consistent with China and Russia's grey-zone warfare strategies**, which seek to weaken opponents through actions which fall just below the threshold of open warfare – often utilising actors with ambiguous and plausibly deniable connections to the state. The suspicious activities of Chinese vessels in Europe, against a backdrop of deepening strategic cooperation between Russia and China, suggests that some level of cooperation between the two countries is plausible – adding further layers of complexity to attribution and denial.

The second section of this paper maps out the UK's risk profile for undersea cable sabotage. As an island nation, the UK is especially dependent on undersea cable infrastructure, both for its international and domestic connectivity. The UK also plays a strategic role in global undersea infrastructure, acting as a key hub for connections between Europe and North America. This means that **the UK's undersea cables could be a prime target for expanding Chinese and Russian grey-zone operations in Europe**, as both actors seek to use non-conventional methods to weaken NATO's defensive capabilities and exploit divisions within the alliance.

The third section of this paper analyses challenges in protecting undersea cables. Measures such as cable burial and steel armouring are insufficient to protect against deliberate sabotage. Monitoring and surveillance is also extremely challenging. While coast guard authorities can use AIS and other data to track and warn vessels encroaching upon restricted zones, the location of undersea cables within busy shipping lanes means that excluding areas near cables is often not possible. Importantly, many monitoring mechanisms fail when ships deactivate or obfuscate AIS data, as demonstrated by a number of cases involving **suspected Chinese and Russian 'shadow fleet' vessels**. Processing large volumes of such data to detect suspicious activity in real time is extremely challenging and necessitates deepened cooperation with likeminded partners.

A further challenge in protecting undersea cables is that pursuing legal accountability for undersea cable sabotage is extremely difficult and compounds efforts to deter potential saboteurs, especially when incidents take place in international waters. UNCLOS places responsibility for investigation and accountability of undersea cable damage on the flag-state of the vessel, not the states impacted by the damage. In practice this means that **states conducting undersea cable sabotage can use international law as a shield against any form of meaningful accountability**. As a result, the UK and its partners must look to alternative mechanisms for accountability – strengthening domestic legislation while also utilising Port State Controls to force investigations and publish blacklists to hold those evading justice to account.

The final section of this report provides recommendations for UK policymakers. There is an urgent need to find innovative ways of protecting undersea infrastructure against emerging threats. While the challenge is complex, the fact that there are only a small number of bad faith actors in this space means that there are ample opportunities to build broad and effective coalitions.

This paper argues that to effectively protect its undersea infrastructure, the UK must work not only with its closest security partners in NATO, but also with likeminded partners in the East Asia region. Taiwan, in particular, has extensive experience of countering maritime greyzone threats, while Japan, South Korea and the Philippines are also looking to develop capabilities. Undersea cables are a global public good, and the normalisation of sabotage as a grey-zone operation threatens security and prosperity everywhere. Efforts to strengthen accountability for undersea cable damage are ineffective without meaningful international cooperation. Bolstering the capabilities of states to protect and strengthen undersea infrastructure – from both deliberate and accidental damage – is in the interests of countries in both regions.

An effective policy response also must engage the private sector, which operates the vast majority of undersea cable infrastructure globally. Undersea cable sabotage puts the huge capital that private companies have invested in undersea cables at risk and hampers the growth of new digital and AI-enabled services. As such, there is a strong incentive for private companies to work with the government to bolster undersea cable resilience, redundancy and repair.

Part One: China and Russia's undersea cable strategy

Suspected incidents of undersea cable sabotage

Undersea cable breakages are not uncommon. According to the International Cable Protection Committee (ICPC), approximately 150-200 submarine cable faults occur each year.[4] Though natural factors such as earthquakes and underwater landslides can cause disruption, the majority of breakages are caused by human activity, such as fishing and anchoring.

A recent rise in damage to undersea cables around geopolitical flashpoints in the Baltic Sea and around Taiwan has raised concerns that some incidents may in fact be acts of deliberate sabotage directed by Russia and China. The table below (page 11-12) lists 12 incidents since 2021 where government agencies have investigated concerns of suspected sabotage against undersea cables. In each case, natural factors have been ruled out as possible explanations, with the main subject of investigations being on identifying the vessel responsible for causing the damage, and whether such damage was caused by negligence or deliberate sabotage. Out of the 10 cases where a suspect vessel has been identified, 8 vessels have direct links to Russia or China through its flag-state registration or ownership.

A few cases are worth highlighting for evidence of particularly suspicious behaviours:

- **Dragging anchors over extended distances:** In the *Newnew Polar Bear* case, the container ship dragged its anchor along the seabed for several hundred nautical miles, causing damage to a gas pipeline and two undersea cables. Similarly, in the *Eagle S* case and *Yi Peng 3* cases, anchors were dragged along the seabed for dozens of nautical miles. It is extremely unlikely that the ship's crew would not notice a dropped anchor and entanglement with cables, which would cause reduced speed for several hours.

- **Irregular movements near cables:** In the *Yi Peng 3* case, the cargo ship was tracked conducting irregular movements, criss-crossing over undersea cables with its anchor down, causing damage to multiple cables in the Baltic Sea.[5] Similar irregular 'zig-zag' patterns were observed in the *Newnew Polar Bear* and *Eagle S* cases.

- **Disabling tracking and obfuscating identities:** The *Yi Peng 3* disabled its transponder over the time period of the incident, preventing the broadcast of AIS data which could be used to track the vessel. This behaviour was mirrored by the *Xingshun 39* case near Taiwan, which switched between two different AIS identities before

[4] Clare, 'Submarine Cable Protection and the Environment'.
[5] Pancevski, 'Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables'.

subsequently disabling AIS to prevent tracking.[6] The *Hong Tai 58* was also found to have disabled AIS broadcasting prior to the incident, and had been registered under multiple identities with the IMO.[7]

- **Ignoring Coast Guard warnings:** In the *Hong Tai 58* case, the vessel ignored seven warnings from Taiwan's Coast Guard instructing it to leave the area near undersea cables around Taiwan's Penghu Islands before cables were severed.

Proving that any individual case is an act of deliberate sabotage is extremely difficult. In many cases suspected vessels have been able to leave the scene without investigation. In the majority of cases where investigations have taken place, most of these have been significantly impeded by limitations on investigation of incidents taking place in international waters, as explored in the next section. At the time of writing, the *Eagle S* and *Hongtai 58* cases are still being investigated by the Finnish and Taiwanese authorities respectively. While these investigations are more promising, it is still highly likely that evidence will still be inconclusive in proving deliberate sabotage over accident or negligence.

However, while individual cases may be difficult to determine, the clear pattern of suspicious activity linked to China and Russia around contested flashpoints around Taiwan and the Baltic Sea, suggests that China and Russia may be integrating attacks on under-sea infrastructure into their broader grey-zone or hybrid warfare strategies. This section analyses these strategies, as well as noting relevant trends and developments in China and Russia's undersea capabilities.

(Table continues on the next page)

[6] The Maritime Executive, 'Chinese Ship Suspected of Cable Sabotage May Have Had Two AIS Devices'.
[7] Wei-li and Chin, 'China Ship Used Taiwan Ports for Months - Taipei Times'.

Table 1: Suspected Incidents of Undersea Infrastructure Sabotage, January 2021 - May 2025

Sources: Compiled by CSRI based on various media reports.

Note: **Gas pipeline; **Power cable*

↓Date	Cable	Location[8]	Jurisdiction	Suspected Vessel		
				Name	Flag	Owner
3/4/2021	LoVe Ocean cable	Norwegian Sea	Norway's EEZ	*Saami*	Russia	Sergei Tsyganov (Russia)
7/1/2022	Svalbard Undersea Cable System	Greenland Sea	Norway's EEZ	*Melkart 5*	Russia	Murman SeaFood (Russia)
26/9/2022	NS1 & NS2*	Baltic Sea	Denmark and Sweden's EEZ	*Andromeda*	Germany	Volodymyr Z. (Ukraine)
2/2/2023	TPKM2	East China Sea	China and Taiwan's EEZ (overlapping claims)	Chinese fishing boat	China	Unidentified
8/2/2023	TPKM3	Taiwan Strait	China's territorial water	Unidentified cargo ship	Unidentified	Unidentified
7/10/2023	Balticconnector* EE-S1 FEC-1	Gulf of Finland	Estonia's territorial water (EE-S1, FEC-1) & Finland's EEZ (Balticconnector)	*Newnew Polar Bear*	Hong Kong	Hainan Xin Xin Yang Shipping (China)

[8] Approximate locations are inferred from public media reports in cases where precise locations of breakages have not been officially disclosed.

17/11/2024	BCS East-West Interlink C-Lion1	Baltic Sea	Sweden's EEZ	*Yi Peng 3*	China	Ningbo Yipeng Shipping (China)
25/12/2024	Estlink2** FEC-1 FEC-2 Baltic Sea Submarine Cable C-Lion1	Gulf of Finland	Finland's EEZ	*Eagle S*	Cook Islands	Caravella LLC-FZ (UAE)
3/1/2025	TPE Cable System	East China Sea	Taiwan's territorial water	*Xingshun 39 (Shunxing 39)*	Cameroon	Jie Yang Trading (Hong Kong)
26/1/2025	Sweden-Latvia	Baltic Sea	Sweden's EEZ	*Vezhen*	Malta	ICBC Leasing (China)
21/2/2025	C-Lion1	Baltic Sea	Sweden's EEZ	Unidentified	Unidentified	Unidentified
25/2/2025	TPKM3	Taiwan Strait	Taiwan's territorial water	*Hong Tai 58*	Togo	Dongguan Jinlong Shipping (Hong Kong)

Undersea cables and grey-zone warfare

Undersea cable sabotage as a grey-zone tactic

Deliberate sabotage of undersea cable infrastructure is consistent with broader 'grey-zone' or 'sub-threshold' coercion strategies deployed by China and Russia.[9] Definitions of grey-zone activities vary, but generally use the term to encapsulate the broad range of activities which fall in the murky space between peace and open conflict.[10] Grey-zone activities are designed to contain significant ambiguity around actors, methods or intent and often make use of non-military means and proxy actors. The most effective grey-zone activities fall just below the threshold of acts of war, maximising the coercive effect while making it difficult for the opponent to respond without escalating into outright war.

> **"Grey-zone activities are designed to contain significant ambiguity around actors, methods or intent and often make use of non-military means and proxy actors."**

In many ways sabotaging undersea cables is an archetypal grey-zone method. Difficulties in monitoring undersea cables means that attributing responsibility for damage is difficult, and even if achieved, there remains significant plausible deniability in claiming that such actions were accidental. Further, attacks on undersea cables can be undertaken by 'shadow fleets' of nominally civilian vessels with ambiguous links to state actors. With limited and ineffective international legal provisions relating to undersea cables, there are no clear routes for escalation or response from the affected state.

China and Russia's grey-zone warfare

The main focus of China's grey-zone operations are on Taiwan, with the goal of undermining Taiwan's autonomy, draining its defensive resources and waging 'cognitive warfare' against its citizens. Sabotage of undersea cables fits well within this model. In the worst incident, the cutting of cables linking Taiwan to its outlying Matsu islands left its 13,000 residents with limited internet access for several weeks.[11] Responding to these threats is expensive.

---

[9] 'Sub-threshold' attacks are generally defined as coercive actions falling just below the legal threshold of 'war', and thus the term is broadly inter-changeable with 'grey-zone' attacks. 'Hybrid warfare' has a slightly different meaning, referring to the combination of grey-zone or sub-threshold activities with conventional military methods.

[10] See Morris et al., 'Gaining Competitive Advantage in the Gray Zone', p. 8: "The grey zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events."

[11] Lii, 'After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience'.

Taiwan's latest budget sets aside NTD 424.67 million (equivalent to USD 13.1 million) on new drones to monitor maritime grey-zone activities.[12] Such incidents also serve as a weapon in China's information operations arsenal, reinforcing Beijing's narratives about the futility of resistance while publicly embarrassing Taiwan's government. In particular, sabotaging undersea cables demonstrates China's ability to severely disrupt Taiwan's communications with the rest of the world in the event of a blockade or attempt to invade Taiwan.

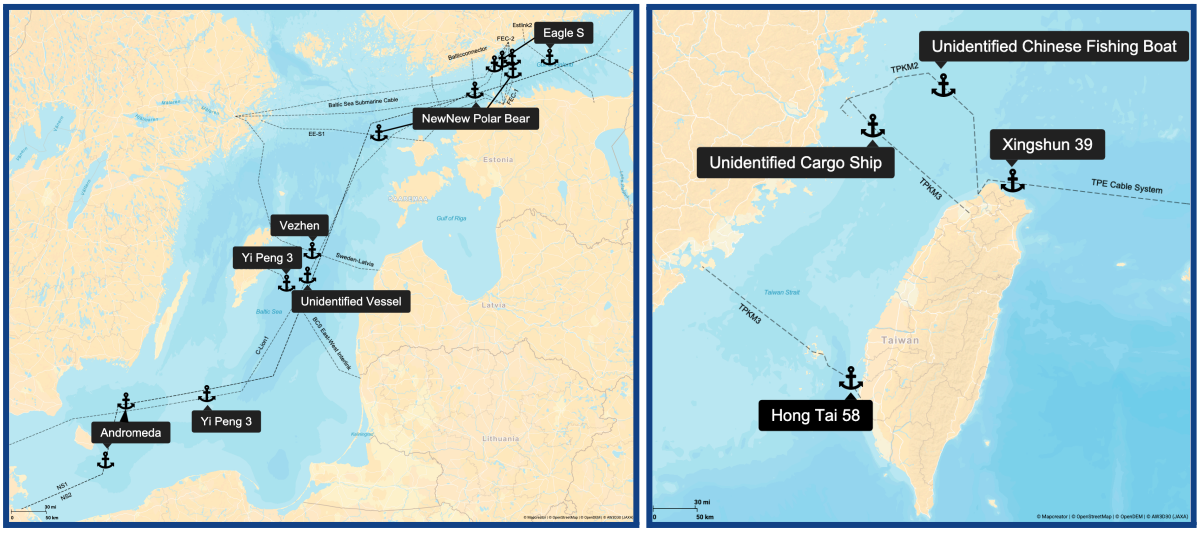


Figure: Incidents in the Baltic Sea and around Taiwan. CSRI Graphics.

China is expanding its grey-zone operations beyond its traditional focus on Taiwan. China's Coast Guard has been deploying increasingly aggressive tactics to assert its territorial claims in the South China Sea, while being careful to keep provocations below the threshold of open conflict. Other grey-zone actions in far-flung locations include live-fire military drills off the coast of Australia and New Zealand and bomber flights around Alaska. While China's grey-zone actions in Europe are more limited, China has conducted extensive cyber-attacks against the UK and other countries, leading to it being labelled as the "dominant" cyber threat by UK officials.[13]

While suspected Russian sabotage operations have so far centered around the Baltic Sea, a strategically important waterway for Russia, the target of such operations is likely to be broader. Undersea cable sabotage is consistent with Russia's broader grey-zone strategy, which is aimed at weakening Europe and undermining NATO. Targeting undersea cables helps Russia map adversaries' critical infrastructure, test response times and develop tactics it could deploy in future conflict scenarios. Threats to undersea infrastructure could also divert NATO members' defensive resources away from the ongoing conflict in Ukraine and other critical areas. The EU has already announced it will spend nearly a billion euros to protect undersea cables, while the JEF's Baltic Sentry Mission has diverted NATO naval resources to the region.[14]

[12] Hsu, 'Taiwan's FY2025 Defense Budget: An Overview of the New Naval Programs - Naval News'.
[13] Wickham, 'UK Cyber Security Chief Names China as Dominant Hacking Threat'.
[14] Reuters, 'EU to Spend Nearly a Billion Euros to Protect Undersea Cables'.

More broadly, undersea cable sabotage could be designed to bolster Russia's attempts to undermine NATO's credibility in Europe. By targeting the Baltic States, Russia may be attempting to drive wedges between member states, particularly at a time when leaders in some NATO countries are questioning the strength and unity of the alliance. Sabotage of critical infrastructure could erode public confidence in NATO's ability to deter threats, giving credence to narratives promoted by Russian information manipulation campaigns.

The growing role of China and Russia's 'shadow-fleets'

Incidents of suspected undersea cable sabotage are also consistent with the growing role of 'shadow-fleets' within China and Russia's grey-zone tactics. So-called 'shadow-fleets' give states the ability to deploy commercial vessels to undertake activities aligning with state-directed coercive objectives, while maintaining the guise of civilian vessels. This gives the state significant plausible deniability, enhancing the ambiguous nature of grey-zone operations.

'Shadow-fleets' have been pioneered by Russia, with analysts estimating that Russia maintains a 'dark-fleet' of up to 1,300 vessels, made up of ships that intentionally disable AIS to transport goods evading international sanctions. This is complemented by a broader 'grey-fleet' of 1,000 vessels operated by companies quickly established in the wake of the Russia/Ukraine war, with opaque ownership structures to evade international sanctions.[15] A number of the Russian merchant vessels suspected of cable sabotage in the Baltic Sea are also thought to be part of Russia's shadow-fleet.

Evidence suggests that China is mirroring Russia's 'shadow-fleet' operations to conduct grey-zone operations around Taiwan. Many of the recent suspected sabotage incidents involved vessels which had multiple registrations, broadcast conflicting identities and disabled AIS transponders for long periods of time, including the *Xingshun 39* and *Hong Tai 58* cases as highlighted above. Taiwan already faces significant challenges from Chinese fishing vessels encroaching into restricted and prohibited waters around Taiwan's outlying Kinmen and Penghu island groups, with many of these vessels also unnamed, unregistered or unlicensed. While illegal fishing has been a long running issue, the recent uptick in encroachments suggests incidents may be part of China's grey-zone activities, with the Taiwanese coast guard having to drive away 567 Chinese boats in the first 6 months of 2024.[16]

Indications of Chinese and Russian coordination on undersea cables

The involvement of a number of Chinese vessels in suspicious incidents in the Baltic Sea, and Russian vessels in the Taiwan Strait, indicates that China and Russia may be cooperating or coordinating attacks on undersea cable infrastructure, with each assisting the other in their respective spheres of influence. Such developments would be consistent

[15] Windward, 'Illuminating Russia's Shadow Fleet'.
[16] Taipei Times, 'Coast Guard Drove Away 567 Chinese Boats in 6 Months'.

with a deepening strategic partnership between Russia and China, with both countries perceiving the Euro-Atlantic and Indo-Pacific as a unified security theatre.

Two Chinese vessels have been at the centre of some of the most egregious cases of suspected undersea cable damage in Europe:

- *Newnew Polar Bear*, a Hong Kong-flagged container ship, identified by Finnish authorities as the suspected culprit of damage to the Balticconnector Pipeline and other undersea infrastructure in October 2023, alongside the Russian flagged *Sevmorput*. The two ships entered and exited the area together, with *NewNew Polar Bear* dragging its anchor for over a hundred nautical miles. Prior to the incident, *Newnew Polar Bear* had called at a number of Russian ports, and had its ownership transferred from a Chinese to a Russian-Chinese company immediately after the incident.[17]

- *Yipeng-3,* a Chinese registered merchant-vessel, identified by Swedish authorities as having severed both the BCS East-West Interlink and the C-Lion 1 cables, linking Lithuania and Sweden and Finland and Germany respectively, after criss-crossing the cables in highly irregular movements.

Both incidents mirror China's tactics around Taiwan, where Chinese-linked commercial vessels have been responsible for damage to undersea cables after dragging anchors across the sea-bed.

Notably, the first reported incident of a Russian ship acting suspiciously near Taiwan occurred in December 2024. The *Vasili Shukshin*, a Belize-flagged, Russian-operated cargo vessel, spent several weeks between December 2024 to January 2025 criss-crossing the area near Taiwan's Fangshan undersea cable landing station, movements which make little sense for its commercial operations.[18] Despite its suspicious behaviour, no damage occurred before its return to a Russian port.

There are a number of shared interests which could motivate coordination between China and Russia on undersea cable sabotage. Carrying out activities in each other's regions allows for both countries to test out grey zone tactics, while adding a further layer of plausible deniability to evade accountability. For China, the ability to project sabotage operations into Europe may also serve as part of warnings against Europe's involvement in any future conflict over Taiwan. Grey-zone operations in Europe could also deter or deplete resources from European countries aiming to increase security engagement in the Indo-Pacific.

While evidence of Chinese and Russian collaboration on undersea cable sabotage in Europe remains uncertain, the growing alignment between China and Russia's strategic goals in undermining NATO, and increasing preference for grey-zone tactics, means that such actions cannot be ruled out in the near future.

---

[17] Dotson, 'Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations'.
[18] Ibid.

China and Russia's deepening strategic partnership

Despite a shared history of rivalry, conflict and mistrust, today China and Russia share a broad interest in undermining what leaders in both countries perceive to be a world order dominated by the West. Both countries see the US as their prime adversary, and undermining NATO – the strongest US-led alliance – as a common goal. China shares Russia's concerns about NATO's eastward expansion, particularly as it pertains to the Indo-Pacific, as well as the growing use of economic statecraft by the US and its allies against their adversaries.

These shared interests are the backdrop to a deepening strategic partnership between Russia and China, in which the Euro-Atlantic and Indo-Pacific are increasingly perceived by both actors as a unified security theatre.

Figure: Dimensions of China-Russia strategic cooperation

President Xi has named China's relationship with Russia as a "no-limits" strategic partnership, and the two nations as being "friends of steel".[19] While China is not directly involved in the war in Ukraine, its support across a number of areas demonstrates its interest in enabling Russia to sustain its war and ultimately reach a conclusion unfavourable to NATO. To this end, China supplies Russia with approximately USD 300 million worth of high priority dual-use products each month, including telecoms equipment, semiconductors and machine tools.[20] At the same time, China has provided an economic lifeline to Russia as it has come under increasing pressure from US and European sanctions, with trade between the two countries 61% higher than before the Ukraine War.[21] China has also sought to bolster Russia's narratives on the Ukraine war, highlighting "Russia's legitimate security concerns" in its 12-points position paper on the "Ukraine crisis" and elsewhere.[22]

There has also been a sharp uptick in the number of joint naval, aerial and coast guard exercises between China and Russia in recent years. Of the nearly 90 joint military exercises since 2003, nearly a third of these have taken place since February 2022.[23] The strategic

[19] Antonov, '"Friends of Steel": Xi and Putin Pledge to Stand Together against US'.
[20] Sher, 'Behind the Scenes: China's Increasing Role in Russia's Defense Industry'.
[21] Soong, 'China-Russia Alignment – a Shared Vision, without Fully Seeing Eye to Eye'.
[22] Sabanadze, Vasselier, and Wiegand, 'China-Russia Alignment: A Threat to Europe's Security | Merics'.
[23] von Essen, 'Joint Military Exercises Signal Deepening Russia-China Strategic Alignment | Merics'.

location of joint exercises suggests an increasing interest in bolstering each other's positions, even outside of their respective regions. Russia has joined China's military exercises in the Yellow Sea, East China Sea and South China Sea, areas critical to China's actions against Taiwan and other territorial claims, but not conventionally perceived as of high strategic importance to Russia. Vice versa, China has joined Russian bomber flights over Alaska, and has undertaken joint counter-terrorism exercises with Belarus – Russia's closest ally in Europe.[24]

China and Russia's enhanced undersea capabilities

Aside from suspected involvement in grey-zone undersea cable sabotage, China and Russia are also bolstering their capabilities to disrupt undersea infrastructure within their conventional military institutions.

Earlier this year the China Ship Scientific Research Centre (CSSRC) and its affiliated State Key Laboratory of Deep-sea Manned Vehicles revealed new technology **capable of severing steel armoured cables at depths of up to 4,000 metres**. The technology is also designed to integrate with existing Chinese manned and unmanned submersibles.[25] This marks a significant development, **giving China the capability to target cables in the deep sea**, which are much harder to monitor than cables in shallow waters, and are generally left unburied and unarmoured. Such capabilities could enable China to extend its cable-cutting operations beyond the Taiwan Strait to the Pacific, Atlantic and elsewhere. Cables cut in the deep sea would pose more complications for repair and replacement than those cut in shallower waters nearer the sea. Other recently developed technologies within China's military industrial complex include algorithmically enhanced robotics to identify cable faults, advanced sonar systems for cable break detection, optical cable retrieval systems and towed cable-cutting systems.[26] While these technologies have some civilian applications, they could also be used to disrupt undersea cable infrastructure as part of grey-zone or war-time tactics if attached to civilian vessels. These developments are part of broader efforts to build China's deep sea capabilities, with "deep sea engineering" named as a priority area in China's 14th Five Year Plan (2021-2025), and "deep sea technology" included for the first time in China's 2025 government work report.[27]

Russia has also developed significant capabilities to map and target undersea infrastructure. Many of these capabilities are contained within Russia's dedicated Main Directorate for Deep Sea Research (GUGI), a specialised branch of the Ministry of Defence that operates separately from the Russian Navy. GUGI is tasked with deep-sea operations, including intelligence-gathering, seabed mapping, and potential attacks on undersea infrastructure.[28] GUGI vessels are equipped with deep-sea submarines and drones capable of operating at extreme depths and conducting detailed surveys and interventions on the seabed, including

[24] Saxena, 'China's Show of Force With Belarus Amid NATO Concerns'.
[25] Chen, 'China Unveils a Powerful Deep-Sea Cable Cutter That Could Reset the World Order'.
[26] Cheung and Yu, 'Creative Destruction: PRC Undersea Cable Technology'.
[27] Herlevi, 'China's Strategic Space in the Digital Undersea - Mapping China's Strategic Space'.
[28] Abramowicz, 'Russian Submarines: Threats and Opportunities for Britain – Britain's World'.

targeting submarine cables and pipelines.[29] GUGI's vessels *Yantar* and *Evgeny Gorigledzhan* have been frequently observed loitering near undersea cables in Europe, along with similar incidents involving the Russian Navy's *Admiral Vladimirsky* off the UK's coastline.

[29] Ryzhenko, 'Russia Looks to Target Achilles' Heel of Western Economies on Ocean Floor | RealClearDefense'.

Part Two: The UK's risk profile

Strategic Importance of the UK's undersea infrastructure

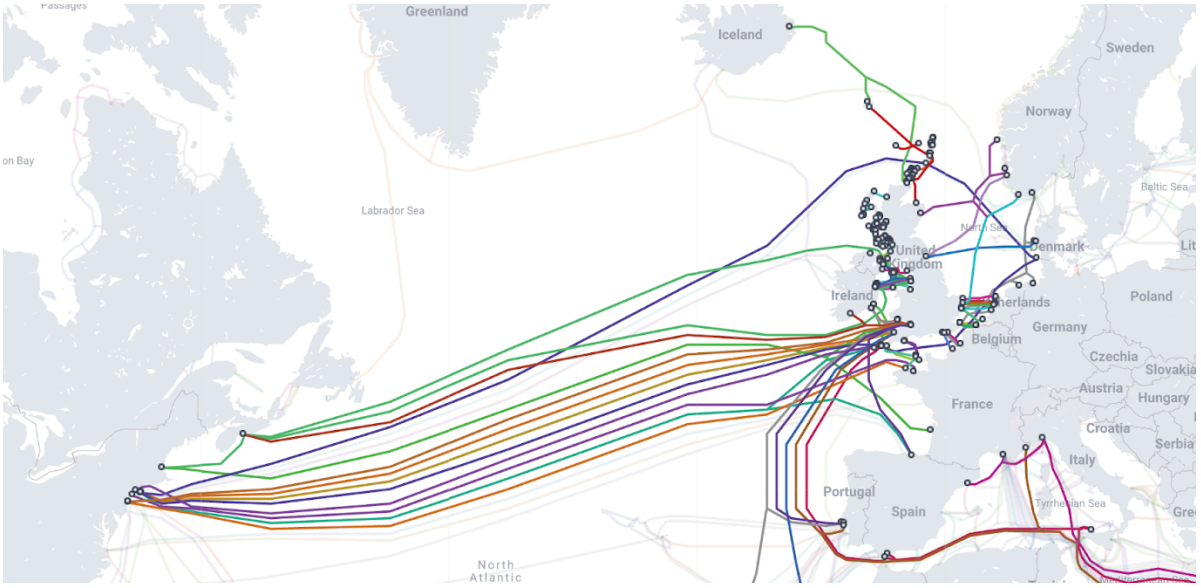


Figure: The UK's undersea cables network[30]

The UK is one of the most important hubs in Euro-Atlantic undersea cable infrastructure, serving as a landing point for over sixty undersea cables – including nine out of the fifteen cables connecting North America to Europe. Aside from North America, other cables landing in the UK connect to Africa, the Middle East and the Asia-Pacific. Notably, a number of these cables are clustered around key landing sites, which increases the risks of several cables being disrupted at once. For example, 9 international cables land in Bude in North Cornwall, and 5 international cables land in Lowestoft in East Suffolk.

As a set of islands, the UK is also highly dependent on undersea cables for its own domestic communications infrastructure. Six undersea cables link Northern Ireland with Great Britain, and more than eleven cables link the UK to its outlying islands and the Crown Dependencies of the Isle of Man, Guernsey and Jersey. Outlying islands such as the Isles of Scilly and the Outer Hebrides are linked to Great Britain by just one undersea cable, meaning that disruption could lead to severe internet outages.

While the significant redundancy in trans-Atlantic and inter-European undersea cable networks means that a total internet black-out is unlikely, disruption to a number of the UK's cables across a short time-frame could have a tangible impact on internet usage, not only in the UK but across Europe and North America. Automatic re-routing of internet traffic to surviving cables could cause congestion, meaning that internet latency (delay) would increase and bandwidth (speed) would reduce. Data-heavy services like video conferencing,

[30] TeleGeography, 'Submarine Cable Map'.

streaming and cloud-based services may see lower performance as a result, with major ramifications across public and private sectors.

Together these factors mean that the UK's undersea infrastructure could be a tempting target for adversaries looking to conduct grey-zone operations against the UK and its allies. The UK's pivotal position in trans-Atlantic communications means that the UK and Europe's undersea infrastructure security is inextricably linked, with the potential for disruption in one area to cause congestion and access issues elsewhere.

Distribution of submarine cables among UK regions and crown dependencies

Data Source: Submarine Cable Map by TeleGeography.[31]

Region	# of Landing Sites	# of Cables (# Intl)	# to Europe	# to North America	# to the Rest of the World
South West England	10	20 (16)	10	8	4
South East England	6	8 (8)	8	0	0
East England	5	9 (9)	9	0	0
North England	3	9 (7)	7	1	0
Scotland	86[32]	11 (3)	3	0	0
Northern Ireland	6	6 (1)	1	1	0
Wales	4	5 (5)	5	0	0
Crown Dependencies	3	8 (2)	2	0	0
TOTAL[33]	123	60 (46)	43	9	4

Threat environment

As analysed in the previous section, China and Russia are actively developing offensive undersea cable sabotage technologies within their military capabilities, while also appearing to deploy undersea cable sabotage by civilian vessels as part of state-directed grey-zone tactics. While the nature of the threat posed by each country is very different, both countries have undertaken a range of actions that demonstrate their continued interest in undermining UK security. Increased coordination between China and Russia could also see an alignment of interests in taking steps to sabotage the UK's undersea infrastructure.

[31] Ibid.
[32] Scotland has a much higher number of landing points due to cables linking its outlying islands, with cables such as R100 North and BT Highlands and Islands Submarine Cable System each having over 30 separate landing points.
[33] Total figures eliminate duplicates whereby one cable system lands in more than one UK region.

Russia: moving from a proxy war to increased grey-zone threats

The UK government's Integrated Review Refresh 2023 designated Russia as "the most acute threat" to the UK's security, posing a range of threats across the domains of nuclear, conventional and hybrid warfare. Significant support provided by the UK to Ukraine's armed forces means that the UK is already engaged in a proxy-war with Russia in Ukraine. While the bulk of Russia's military resources are currently concentrated on its war with Ukraine, increasing prospects of a ceasefire could allow Russia to re-divert these resources to bolster its grey-zone strategy against other countries in Europe – including the UK.

Targeting the UK's undersea infrastructure could help Russia meet a number of strategic objectives. Firstly, such actions could test and undermine NATO's credibility at a time when its internal cohesion is already under considerable strain. Secondly, undersea cable sabotage could divert the UK and other NATO member states' defensive resources away from other priorities, including proposed European security initiatives and peace keeping forces in Ukraine. Finally, these actions could also serve as a warning against the UK from taking actions against Russia's interests in other domains.

Russian vessels have already been observed near the UK's undersea cable infrastructure. The Russian spy ship *Yantar* was escorted out of British territorial waters in November 2024 after being observed "loitering over UK critical undersea infrastructure", and then again in January 2025.[34] In both cases the vessel was suspected of undertaking a mapping of the UK's undersea infrastructure, though no damage occurred. While the Russian navy does undoubtedly have the capabilities to sabotage the UK's undersea infrastructure, it is more likely that sabotage would be undertaken by a commercial vessel. This would be in keeping with Russia's grey-zone strategy, allowing it to achieve its objectives while retaining significant ambiguity and plausible deniability over its actions. Russia's extensive and opaque shadow-fleet would be an important asset for Russia should it decide to follow such an approach.

China: undermining the UK's security alliances

While China does not pose as direct a threat to the UK as Russia, it still has a strategic interest in undermining the UK's security. China views its chief adversary as the US, which it sees as acting to constrain China militarily, economically and technologically. The close military and intelligence relationship between the US and UK has seen China take a strong interest in compromising the UK's security. The UK is a frequent target of China's espionage attempts, while UK intelligence services have identified China as the "dominant" source of cyber-attacks against the UK, posing a "significant risk" to critical infrastructure.[35] [36] China's threats are not limited to the military domains but extend into the UK's civilian domain, with suspected Chinese state-backed cyber-attacks including the Ministry of Defence, Foreign Office, Electoral Commission and a number of NGOs. **While targeting undersea infrastructure would mark an escalation of attacks from the cyber to the physical domain, it**

[34] Panella, 'A British Submarine Secretly Tracking a Russian Spy Ship Hanging around Undersea Cables Surfaced Close to It to Send a Message, UK Says'.
[35] Wickham, 'UK Cyber Security Chief Names China as Dominant Hacking Threat'.
[36] National Cyber Security Centre, 'NCSC Annual Review 2024'.

would be consistent with China's demonstrated willingness to test and compromise the security of the UK's critical infrastructure.

Aside from its rivalry with the US, China has demonstrated an increasing interest in checking the activities of NATO more broadly. China has repeatedly voiced opposition to NATO's increasing engagement with the Indo-Pacific, which it sees as a further extension of US attempts to push back against China's influence and territorial claims in the region. Most recently, a joint statement issued by President Xi Jinping and Russian counterpart Vladimir Putin on the 80th anniversary of VE day warned European countries against efforts to extend influence in the Indo-Pacific.[37] China and Russia have expressed similar joint opposition to AUKUS, of which the UK is a part.[38] China's support for Russia's war in Ukraine – including exports of dual-use technologies, as well as importing large amounts of Russian oil and gas – can broadly be interpreted as strategic alignment with Russia's attempts to weaken NATO in Europe.

Targeting of the UK's undersea cable infrastructure could thus help China meet a number of objectives, including:

- Undermining NATO by challenging its credibility and draining its defensive resources.
- Diverting the UK and NATO's attention away from the Indo-Pacific.
- Testing the readiness and response capabilities of the UK and NATO.
- Warning the UK and other European countries against challenging China's interests, for example, in the event of any future conflict over Taiwan.
- Providing support to Russia's objectives, either in exchange for favours in other areas, or out of strategic alignment with Russia's goals under their 'no-limits' partnership.

As with Russia, it is likely that any such actions would be undertaken as a grey-zone operation, with civilian vessels leveraged to maximise uncertainty. Initial actions may seek to 'test the waters' to gauge the UK's response, before escalating to more serious damage.

[37] Hawkins, 'China and Russia Pledge to Deepen Ties as They Criticise US on Victory Day'.
[38] Roth and Ni, 'Xi and Putin Urge Nato to Rule out Expansion as Ukraine Tensions Rise'.

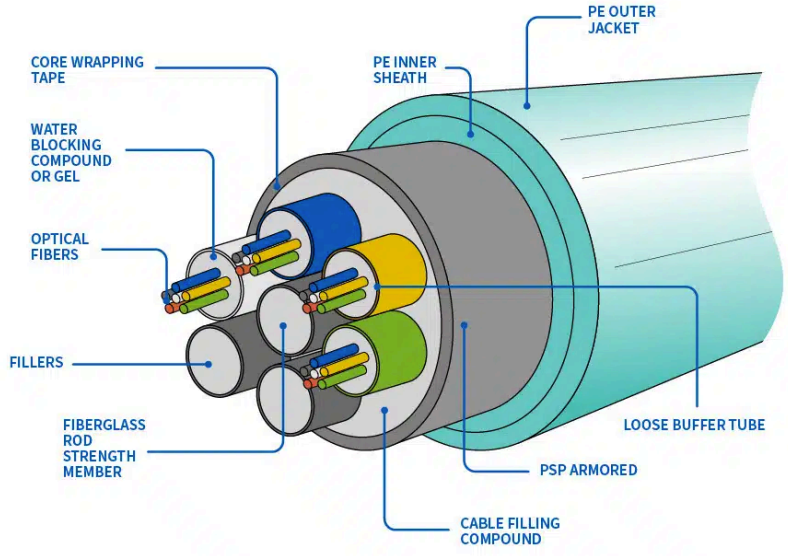
Part Three: Challenges in protecting undersea cables

Undersea cables are an attractive grey-zone target because they are far more vulnerable than other forms of critical infrastructure. Undersea cables are typically just 17-25mm thick, roughly the same size as a garden hose. Beyond water-proofing, steel wiring and plastic sheathing, there is little else to protect the thin glass optical-fibres within. Cables in shallow or busy waterways can be given additional protection in the form of steel armouring or burial below the sea-bed – typically at a depth of 1-3 metres. However, burial and armouring are not sufficient to guarantee protection against damage from anchors and other common shipping equipment. Although data is not publicly available in each instance, the majority of incidents of suspected cable sabotage are believed to have cut cables which had been buried and/or armoured, including all of the incidents involving Taiwan.

This section examines a number of factors which compound the challenges of protecting undersea cable infrastructure from deliberate sabotage. The location of undersea cables in busy sea lanes makes monitoring and surveillance of undersea infrastructure extremely challenging. Undersea cables also suffer from a number of loopholes in international law, meaning those who damage them are unlikely to be held to account. Vulnerabilities are further compounded by a global shortage of cable repair vessels, meaning that breaks can take months to fix.

The anatomy of a fibre optic cable

Source: Ripley Tools.[39]



[39] Ripley Tools, 'Taking a Closer Look at the Anatomy of a Fiber Optic Cable'.

Monitoring difficulties

Monitoring which vessels might pose a danger to undersea cables is a major challenge. The UK's undersea cables traverse some of the world's busiest sea lanes. The majority of connections between the UK and Continental Europe traverse either the North Sea or the English Channel – which see 7,600 and 400 ships passing through each day respectively.[40] [41] The Irish Sea, which many of the UK and Ireland's transatlantic cables connect through, sees more than 1.6 million freight shipments a year.[42] Though access is restricted around areas near key landing points, there is no way of diverting maritime traffic away from undersea cables entirely. This makes identifying vessels posing a threat to undersea cable infrastructure difficult and resource intensive – particularly given the extensive use of ordinary commercial vessels to conduct sabotage.

The UK deploys a broad array maritime domain awareness technologies, with institutions in place to coordinate intelligence sharing across government. The Royal Navy's Maritime Domain Awareness Programme (RN MDAP) is the UK's primary advanced vessel monitoring system. This draws upon several sources of information, such as the Automatic Identification System (AIS), coastal radar, and regional vessel detection agreements. This, along with other information from agencies including the UK Border Force, Maritime and Coastguard Agency and police forces feeds into the National Maritime Information Centre (NMIC) within the Joint Maritime Security Centre (JSMC), the multi-agency organisation responsible for monitoring threats to security, law and order in the maritime domain.[43]

However, by the UK government's own admission, the UK has limited capabilities for monitoring general maritime traffic, including commercial and civilian vessels. Coastal radar only covers about 22 percent of the Exclusive Economic Zone (EEZ) around the UK, while the high volume of maritime traffic makes it challenging to identify every instance of abnormal maritime activity.[44] This means that the UK's maritime domain awareness infrastructure is inadequate to meet the grey-zone nature of threats to its undersea infrastructure, with all suspected incidents to date being undertaken by regular commercial ships. **While the UK's infrastructure is well set up to guard against conventional military threats, identifying and tracking prospective grey-zone threats among the many thousands of legitimate vessels operating in UK waters remains the key challenge for protecting undersea infrastructure**.

The UK is increasingly looking to new technologies to enhance its data collection and analysis capabilities, including against grey-zone threats. In January 2025, the UK-led Joint Expeditionary Force (JEF) *Nordic Warden* mission deployed AI driven data analysis tools to assess AIS and other sources of data to calculate the risk posed by each vessel entering areas near undersea cable infrastructure.[45] These efforts have complemented NATO's *Baltic*

[40] Henrik Nilsson et al., 'Transnational Maritime Spatial Planning in the North Sea: The Shipping Context'.
[41] Lock, 'Geo Explainer: Where in the World Are the Busiest Shipping Lanes?'
[42] Freightlink, 'Irish Sea Ferry Routes'.
[43] Systematic, 'SitaWare Delivers Situational Awareness of UK Waters'.
[44] UK Government, 'Written Evidence Submitted by HM Government to the Questions Posed in the Joint Committee for National Security Strategy's Call for Evidence on Undersea Cables.'
[45] Ministry of Defence et al., 'Joint Expeditionary Force Activates UK-Led Reaction System to Track Threats to Undersea Infrastructure and Monitor Russian Shadow Fleet'.

Sentry mission, also launched in January 2025, which aims to improvise integration of surveillance assets between member states.[46] The UK also has plans to deploy:

- The Lura system, an AI-driven network of autonomous underwater gliders.[47]
- The Amber-2 Maritime Domain Awareness (MDA) Satellite, which will track and monitor 'dark vessels' that turn off their AIS to evade detection.[48]
- Underwater drones and other capabilities through RFA Proteus, the UK's first Multi-Role Ocean Surveillance Ships (MROSS). However, previously announced plans for a second vessel are reportedly still delayed at the "concept phase".[49]
- Distributed Acoustic Sensing (DAS) technologies for undersea cables, in partnership with cable operators.[50]

While the UK has made significant progress in its monitoring capabilities it still has much to gain from deepening exchange with other governments that have extensive operational experience in this area. Notably, **the UK should be learning from Taiwan's extensive experience in monitoring and responding to suspicious vessels** posing a threat to undersea infrastructure. Taiwan is developing new inter-agency coordination protocols to respond to incidents, including developing early detection systems with telecommunications providers, and is considering deploying Synthetic Aperture Radar (SAR) systems to complement AIS based monitoring systems. Exchanges between the UK and Taiwan could focus on sharing experience and best practice in data analysis, deployment of new technologies, and inter-agency coordination. Given the prospect of increasing grey-zone cooperation between Russia and China, the UK can benefit from Taiwan's intelligence on China's expanding shadow fleet and maritime capabilities, while Taiwan could benefit similarly from the UK's intelligence on Russia. Japan, which is developing underwater drones that can patrol cable routes, South Korea and the Philippines are also like-minded partners that are facing many of the same challenges as the UK.[51]

Limited legal accountability

Pursuing accountability for acts of damage to undersea infrastructure within the UK's territorial waters is possible under the UK's Submarine Telegraph Act 1885, which criminalises the wilful or culpable negligence of undersea cables. However, avenues to pursue legal accountability for acts of damage against undersea cables outside of territorial waters are extremely narrow and hampered by a number of long-standing limitations to the law of the sea. As shown in Table 1 (page 11-12), the majority of suspected sabotage

[46] NATO, 'NATO Launches "Baltic Sentry" to Increase Critical Infrastructure Security'.
[47] NavyLookout, 'AI-Enabled Underwater Gliders Could Enhance Royal Navy ASW Capability | Navy Lookout'.
[48] UK Space Agency, 'UK Satellites to Boost Maritime Security on Track for 2025 Launch'.
[49] Allison, 'MoD Tight-Lipped on Second Undersea Surveillance Ship'.
[50] Alcatel Submarine Networks, 'Written Evidence Submitted by Alcatel Submarine Networks: Use of Fibre Sensing to Secure UK Subsea Infrastructure'.
Indeximate Ltd, 'Written Evidence Submitted by Indeximate Ltd: Monitoring the Health and Security of Undersea Infrastructure'.
Crosslake Fibre UK Limited, 'Written Evidence Submitted by Crosslake Fibre UK Limited'.
[51] Abke, 'Indo-Pacific Nations Bolstering Defense of Undersea Cables against Emerging Vulnerabilities'.

incidents take place outside of a country's territorial waters, which stretches just 12 nautical miles from the coastal baseline.

The UK is party to the 1884 Convention for the Protection of Submarine Telegraph Cables (Paris Convention), which declares willful or culpably negligent damage to subsea cables a punishable offense. The Paris Convention does permit any signatory nation to inspect vessels belonging to other signatory nations that are suspected of damaging submarine cables. However such inspections are restricted to requesting the vessel's captain to produce official documentation proving the vessel's nationality, and does not allow inspectors to make arrests. The small number of countries that have signed the Paris Convention also limits its usefulness against undersea cable sabotage. While the 36 signatories include Russia, it does not include China, nor Cameroon, Togo or other common so-called 'flags-of-convenience' countries whose vessels have been involved in suspected incidents.

Provisions with UNCLOS are similarly limited. Unlike the Paris Convention, UNCLOS has been ratified by a much broader set of countries, including Russia and China. Similarly to the Paris Convention, UNCLOS allows states to adopt necessary laws and regulations to protect subsea cables within their territorial waters.[52] However, specific references to undersea cables outside of territorial waters UNCLOS are limited to Article 113, which requires signatories to penalise vessels flying under their flag that are engaged in the willful or culpably negligent damage of subsea cables outside of their territorial waters.

These provisions align with the underlying principles of UNCLOS, chiefly the exclusive jurisdiction given to flag states over their ships on the High Seas.[53] In practice, this means that, in the case of undersea cable damage on the High Seas, no arrest or detention of the ship can take place without the authorisation of the flag state. Further, only the flag state (or state of nationality) can institute proceedings against the crew of the ship in such an event. Should the state suffering the cable break believe the flag state has not asserted proper jurisdiction or control over one of its flag vessels, its actions are limited to reporting the matter to the flag state, which is then responsible for investigating the matter, and taking action if appropriate.[54]

International conventions on undersea cable protection

Law / Article	What it says	Limitations
Paris Convention (1884)	- Damaging cables outside territorial sea is a punishable offence - Contracting parties can inspect suspect merchant vessels in international waters	- Investigatory powers are limited - Only 36 countries are parties, excluding China

[52] United Nations, 'United Nations Convention on the Law of the Sea'.
[53] Ibid., supra note 23, art. 92.
[54] Pedrozo, 'Safeguarding Submarine Cables and Pipelines in Times of Peace and War'.

UNCLOS Article 21	- Coastal states may adopt laws to protect cables within their territorial sea	- Most cable cuts happen outside territorial waters
UNCLOS Article 113	- Countries shall punish vessels flying their flag for wilful or negligent cable damage outside territorial waters	- Enforcement relies on the flag state, not the victim - Hard to prove intent - Flag states often don't act

By delegating enforcement to the flag-state, UNCLOS provisions on undersea cables suffer from a number of obvious loopholes. **UNCLOS puts the responsibility on the state of the suspected perpetrator to hold violators to account, rather than that of the victim.** A number of recent cases demonstrate how this system fails to provide meaningful accountability, allowing flag-states to block investigations by other states, or conduct their own investigations on terms favourable to its own interests, with limited or no input from the victim state.

- In the *Yi Peng 3* case, Swedish investigators were initially denied permission to inspect the vessel by China. By the time permission was granted, the ship's Voyage Data Recorder (VDR) had already overwritten the relevant recordings, and investigators were not given access to onboard surveillance footage.[55] Swedish investigators eventually concluded that they did not have the evidence to make a judgement on the nature or intent of the incident.

- In the *Newnew Polar Bear* case, Chinese authorities did investigate the case themselves, but did not allow meaningful participation from Finnish, Estonian and other investigators. The Chinese investigation concluded that the Hong Kong vessel had severed the cables accidentally, with the captain later charged by the Hong Kong authorities with reckless criminal damage and minor regulatory infringements, with penalties under the latter limited to light fines.[56] While the case is ongoing, the declining independence of Hong Kong's legal system and the removal of the opposition from its Legislative Council will limit opportunities for thorough scrutiny and accountability. This is a growing problem given Hong Kong's role as a global hub for vessel registration.

Prospects for accountability under UNCLOS

Prospects for accountability against Russia and China rest on more general legal principles underpinning UNCLOS. Russia and China due to their repeated failure to take appropriate action against the ships, their masters and crew, involved in damaging undersea cables, are violating their good faith obligations under UNCLOS, namely that they should "fulfill in good faith the obligations assumed under this Convention and shall exercise the rights, jurisdiction and freedoms recognized in this Convention in a manner which would not constitute an abuse of right." **The UK should publicly signal its dissatisfaction at Russia and**

[55] Wodecki, 'Sweden Finds No Proof Chinese Ship Cut Baltic Cables on Purpose'.
[56] Hioe, 'Another Severed Submarine Cable Raises Alarm in Taiwan'.

China's failure to fulfill their good faith obligations under UNCLOS, either through UNCLOS or other forums. The UK should also voice its support for like minded partners such as Estonia, Sweden, Finland and Taiwan as they continue to pursue accountability for suspected undersea cable sabotage, and should actively counter any attempts by Russia and China to portray such actions as contrary to international law.

An alternative route towards accountability within existing frameworks is **the use of port state jurisdiction to investigate and report suspected vessels**. Under UNCLOS, states have sovereign jurisdiction over vessels docking in their ports. Port authorities are able to exercise this jurisdiction to conduct Port State Control (PSC) inspections on vessels, which ensure adherence with international maritime laws and safety standards. The UK, along with most other European countries, is part of the Paris Memorandum of Understanding on Port State Controls (Paris MoU), which standardises PSC inspections and shares information collected between its members. Notably, the Paris MoU regularly publishes Ship Risk Profiles, which compile data on individual vessels' inspection history, deficiencies, and detentions, and the Flag State Performance List, which compiles data on the compliance record of flag states based on the performance of their registered fleets.

The UK could push for Paris MoU members to **establish a joint investigation and reporting mechanism for vessels suspected of undersea cable damage**, prompting targeted PSC inspections. Investigations could examine patterns of anchoring, trawling, or transiting in protected cable zones for evidence of reckless or malicious behaviour. Data on the number of cable incident related inspections, and subsequent compliance with such inspections, can then be published by the Paris MoU, either through integration into existing the Ship Risk Profiles and Flag State Performance List or separately.

Alternative routes to accountability

While existing routes to accountability remain limited, the UK should urgently work with a broad set of international partners to **establish new norms of lawful and proportionate countermeasures** against vessels suspected of undersea cable sabotage. Measures should include agreeing on joint protocols for the rapid interdicting or seizing of suspected ships and crew.[57] Such protocols should allow for the use of non-lethal force in cases of non-cooperation, such as non-consensual boarding, warning shots, nets and traps, in accordance with the principles of the UN Charter.[58] Common protocols could be codified through NATO, or extended to a broader set of like minded countries including Japan, Taiwan, South Korea, Australia and New Zealand.

To be effective, such protocols should not be confined to incidents taking place inside the UK's territorial waters, but be extended to its EEZ. The UK should seek to use existing domestic legislation to grant the legal basis for such actions. The National Security Act 2023 (NSA) already criminalises sabotage against the UK's infrastructure, if conducted on behalf of a foreign power, including for actions outside of the UK. The UK government could pre-emptively signal that it would be willing to **use the NSA to target suspected grey-zone saboteurs of undersea infrastructure**, including for incidents taking place outside of the UK's

[57] Pedrozo, 'Safeguarding Submarine Cables and Pipelines in Times of Peace and War'.
[58] Article 2(4). From ibid.

territorial waters. Alternatively, the Submarine Telegraph Act 1885 could be updated to reflect modern maritime zones, namely clarifying that its provisions apply not just to the UK's territorial waters but also its EEZ and continental shelf.[59] Such actions would be in line with those taken by other countries, with Estonia's new laws criminalising damage to undersea infrastructure, including in its EEZ.[60]

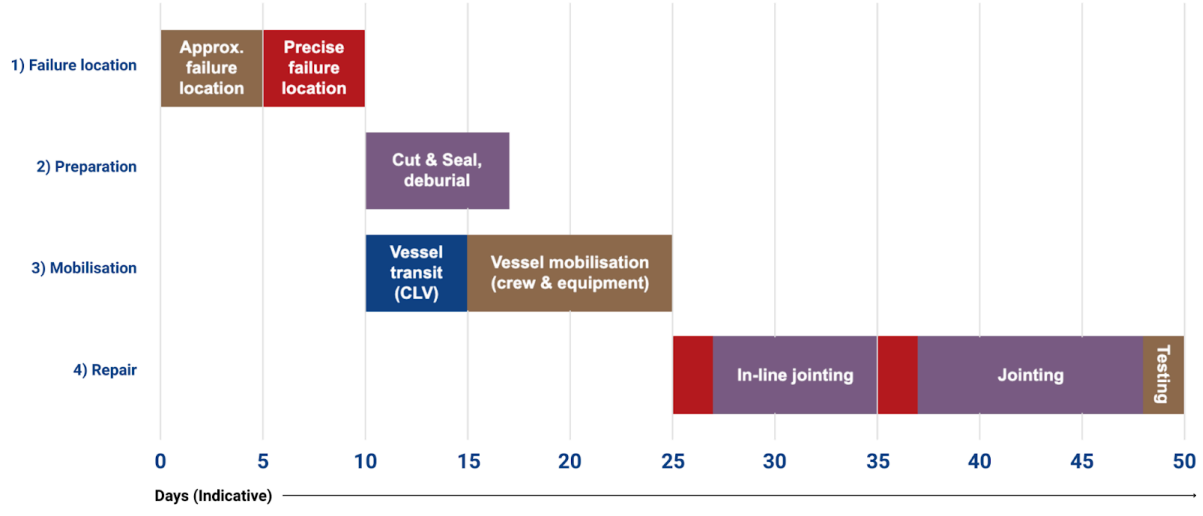
Costly and lengthy repair

The cost and length of repairs compound the vulnerabilities of undersea cables, with global shortages of specialised personnel and equipment a major factor.

Failure identification in itself can be a time consuming process, often taking several weeks. Successful failure identification is generally reliant on accessibility to specialist ROV equipment to discover and locate breakages. Once identified, the next phase of repair requires the use of cable-laying vessels (CLVs) to remove and replace the faulty section. CLVs are in short supply globally, with approximately only 60 commercially available CLVs listed on the International Cable Protection Committee registry.[61] Despite their critical importance, the cable repair industry has run on low profit margins and has not attracted many newcomers. As a result, the global CLV fleet is small and aging, with no new build cable ships delivered between 2004 and 2010, and only five ships delivered between 2011 and 2020.[62] This means that it can take weeks or even months for CLVs to become available and travel to the location of the breakage.

A timeline of locating undersea cable failures

Source: Spinergie.[63]



All of the undersea communications cables landing in the UK are operated by private companies, each of which have their own repair and maintenance arrangements through the

[59] Hartmann, 'Written Evidence Submitted by Dr Jacques Hartmann, Professor in International Law and Human Rights, University of Dundee'.
[60] The Baltic Times, 'Estonia Tightening Criminal Law to Protect Underwater Infrastructure'.
[61] International Cable Protection Committee, 'Cableships of the World'.
[62] Submarine Telecoms Forum, Inc, 'Industry Report 2021/2022'.
[63] Spinergie, 'How offshore cable repair operations impact the market'.

Atlantic Cable Maintenance Agreement (ACMA) or the Atlantic Private Maintenance Agreement (APMA). These agreements have limited provision for emergency repairs:

- ACMA maintains three cable repair vessels on 24/7 call for emergency repairs in the North Atlantic.[64] Global Marine Systems, a UK company and key repair provider under ACMA, maintains several CLVs with a baseport in the UK. However, there is no preferential availability to UK ACMA members.[65]

- APMA pairs individual cable operators with two APMA maintenance contractors, Alcatel Submarine Networks (ASN) and TE Subcom. The speed and availability of APMA's repair fleets for individual operators varies according to the specific agreement negotiated.[66]

Availability of Commercial CLVs by baseport country

Source: Submarine Telecoms Forum, Inc.[67]

Baseport Country	No. of CLVs
United States	5
United Arab Emirates	5
United Kingdom	4
France	4
China	3
Japan	3
Taiwan	2
Rest of the World	32

In practice this means that **the UK government does not have direct control over how quickly the UK's submarine cables are repaired**, and how quickly the UK's internet service is restored in the event of disruption**.** The UK's cable infrastructure is instead reliant on the quality of individual arrangements made by cable operators. While the existing agreements may be sufficient for routine levels of undersea cable damage, they are not sufficient to address large-scale sabotage in grey-zone or conflict scenarios. For example, a coordinated cable cutting operation across the North Atlantic could very quickly deplete the emergency repair fleet of three vessels maintained by ACMA.

To address this challenge the UK government should make arrangements for guaranteed repair fleet availability in crisis scenarios. While RFA Proteus, the first of the Royal Navy's Multi-Role Ocean Surveillance Ships (MROSS), does have some repair capabilities, its dual

[64] UK Government, 'Written Evidence Submitted by HM Government to the Questions Posed in the Joint Committee for National Security Strategy's Call for Evidence on Undersea Cables.'
[65] Webster, 'ACMA 2017 Agreement Extended to the End of 2025 With Suppliers Global Marine and Orange Marine'.
[66] Offshore Energy, 'ASN, TE SubCom Get Telefónica Maintenance Contract Extension'.
[67] Submarine Telecoms Forum, Inc, 'SubTel Forum Submarine Telecoms Industry Report'.

role as a surveillance and reconnaissance ship means that it could be impractical to use it for purposes of repair during a crisis. The UK government could emulate the arrangements with private firms made by the US government, which has secured an agreement with Subcom to establish the Cable Security Fleet, whereby the government has continuous access to two SubCom cable repair vessels in case of a national emergency for $10 million annually. Alternatively, the UK government could seek to enter into agreements with the EU to maintain a joint repair fleet. The EU Action Plan on Cable Security has proposed the establishing of a multi-purpose EU Cable Vessels Reserve Fleet to be used in case of emergency, to deploy or repair electric or optical submarine cables connecting EU territories, while contracting commercially available services in the meantime.[68]

[68] European Commission, 'Joint Communication to Strengthen the Security and Resilience of Submarine Cables | Shaping Europe's Digital Future'.

Conclusion

Undersea cables must be treated as a global public good. An attack on one is, in effect, an attack on the entire system. While individual nations may oversee specific cable segments, the strategic and economic fallout from any successful interference is shared across borders. More broadly, the normalisation of grey-zone attacks on undersea cables has a global impact, making all critical digital infrastructure more vulnerable.

Fortunately, the number of suspected bad-faith actors in this domain remains limited, with Russia and China the major culprits so far. This creates space for an opening for the UK to build broad coalitions among like minded states, including but not limited to its long-standing security partnerships through NATO. Taiwan, Japan, South Korea and other East Asian countries, many of which face the same challenges as the UK, are promising partners in this field.

This report identifies three main areas where the UK can enhance work to strengthen the security of its undersea cable infrastructure, with a particular focus on the benefits of international cooperation.

The most immediate and urgent area for cooperation is **enhancing joint monitoring and surveillance capabilities.** Monitoring systems can play an early-warning preventive role, while effective data collection in relation to incidents is essential for aiding subsequent attempts at accountability. As threats from Russia and China's 'shadow-fleets' grow, working with likeminded partners in Europe and Asia to improve intelligence and best practice can be extremely beneficial.

Secondly, the UK should work with its partners to **strengthen accountability mechanisms** for undersea cable damage. Rather than serving as an effective mechanism for accountability, UNCLOS has enabled Russia and China to obfuscate or refuse investigations and deny responsibility. Countries should use existing powers such as the Paris MoU and domestic legislation to hold saboteurs to account, as well as codifying new protocols to pursue, interdict and detain suspected vessels, even when such incidents happen outside of territorial waters.

Finally, the UK must work with industry stakeholders to **improve redundancy, resilience and repair** in new and existing undersea cable networks. Ensuring that cables can be repaired quickly and efficiently helps safeguard cables from both deliberate and accidental disruption. This safeguards the interests of private sector stakeholders – not just those operating cables, but also digital, tech and other industries who rely on undersea cable development.

Policy Recommendations

(1) Enhancing monitoring and surveillance

- **Data sharing and analysis:** The UK should establish forums with partners for sharing data on the identity and activities of ships which may pose a risk to undersea cables, including those believed to be within Russia and China's 'shadow-fleets'. Data shared could include AIS data, ship registration data, ownership data, port call data and satellite imagery. In particular, the UK should establish data sharing mechanisms on a bilateral level with Taiwan, which has devoted significant resources to such analysis, as well as Canada, Japan, South Korea and other partners. The UK should also seek a role in EU proposals for an Integrated Surveillance Mechanism for Submarine cables as part of ongoing discussions on the UK–EU Security and Defence Partnership. Such forums should also integrate data from private sector sources, such as cable operators and the shipping industry.

- **Exchange of best practice:** The UK should conduct regular engagements with partners to exchange best practice on undersea cable monitoring and surveillance. Discussions could focus on areas such as use of early warning systems and other technologies, data collection and analysis (including AI-driven behavioural analytics), inter-agency cooperation, war gaming and rapid response tactics. Such exchanges could take place through relevant diplomatic or representative offices, or with partners including Japan and Taiwan through the Global Cooperation and Training Framework. Regular exchanges could also help open effective channels for communication and coordination in future crises.

- **Joint exercises and patrols:** The UK should continue to play a leading role in NATO and JEF exercises and drills focussing on the surveillance and protection of undersea infrastructure, as well as considering including these operations as part of ongoing discussions within the UK–EU Security and Defence Partnership. Future exercises could focus on practising skills such as interdicting or boarding vessels suspected of undersea cable damage. While joint exercises and patrols are unlikely to be frequent or extensive enough to make a major contribution to surveillance, they can still play an important deterrent effect by demonstrating capabilities and showing united international support. Future deployments of UK vessels to the Indo-Pacific could include joint exercises and patrols with undersea infrastructure as a focus.

(2) Strengthening mechanisms for accountability

- **Publish blacklists of offending vessels:** The UK should publish regularly updated blacklists of vessels involved in incidents of undersea cable sabotage and suspected vessels evading investigators. For maximum impact, such blacklists should be published in coordination with likeminded partners such as the EU or G7. Such lists

could simply 'name and shame' offending vessels, with likely impacts on the designated vessels' commercial operations, or be further strengthened by sanctions and punitive measures against those listed. Sanctions could include preventing blacklisted vessels from entering ports, insurers or other service providers in that country, or asset freezes against the vessel owners and operators, as provided for under the UK's Sanctions and Anti-Money Laundering Act.

- **Amend the Paris MoU to incorporate cable-related compliance criteria:** The UK should lead efforts to amend the Paris Memorandum of Understanding on Port State Control – of which it and most European countries are parties – to integrate cable-related incidents into ship risk profiles. This should include establishing an agreed reporting mechanism where coastal states alert Paris MoU members of cable incidents tied to specific vessels, prompting targeted PSC inspections. Investigations could examine patterns of anchoring, trawling, or transiting in protected cable zones for evidence of reckless or malicious behaviour. Data on the number of cable incident related inspections, and subsequent compliance with such inspections, can then be integrated into existing Ship Risk Profiles and the Flag State Performance List published by the Paris MoU.

- **Establish Joint Protocols for Pursuit and Investigation:** The UK should work through NATO or other partnerships to adopt protocols allowing for the rapid pursuit, interdiction and detention of vessels suspected of cable damage. This should include the legitimate use of non-lethal, limited force against non-cooperative or evasive vessels in a manner consistent with the UN Charter. Examples of such measures could include the use of non-consensual boarding, non-lethal disabling technologies (such as entanglement nets or propeller traps) and warning shots. Publicly codifying procedures will both serve as a deterrent and demonstrate that responses are proportionate and consistent.

- **Amend domestic legislation to extend jurisdiction:** The UK should update its domestic legislation to allow for extension of penal jurisdiction to its Exclusive Economic Zone for cases in which there is credible suspicion of damage to the UK's critical undersea infrastructure. This could be achieved through updating the Submarine Telegraph Act 1885 to reflect modern maritime zones, namely clarifying that its provisions apply not just to the UK's territorial waters but also its EEZ. This could also be achieved through signalling that the UK would be willing to use the National Security Act 2023, which already criminalises sabotage against the UK's infrastructure conducted on behalf of a foreign power and is already extraterritorial in nature, for cases of suspected sabotage against the UK's undersea cables.

- **Increase diplomatic pressure on non-cooperative flag states:** Governments can put diplomatic pressure on China, Russia and other countries that fail to meet their good-faith obligations under UNCLOS to take meaningful measures to investigate and hold perpetrators of undersea cable damage to account. Such pressure could take place in established UNCLOS forums or through bilateral channels. Such an approach could be particularly effective for smaller, so-called 'flags of convenience'

states. While many of these states gain from operating a light-touch regulatory model, they may still have some diplomatic and economic incentives to maintain a reliable reputation. It is likely that many of these countries have not chosen to take part in Russia and China's shadow-fleet or grey-zone operations, and with the right diplomatic pressure, could be persuaded to distance themselves from these activities through ensuring meaningful investigation and accountability.

(3) Improving redundancy, repair and resilience

- **Ensure UK access to cable repair vessels in crisis scenarios:** The UK government should secure guaranteed access to cable repair vessels to ensure rapid response capability during crises or national emergencies. While the Royal Navy's new Multi-Role Ocean Surveillance Ship, RFA Proteus, has some repair capability, its primary surveillance function could limit its availability for cable repair during emergencies. The UK should consider emulating the United States' model, where the government pays SubCom $10 million annually for continuous access to two cable repair vessels through its Cable Security Fleet. Alternatively, the UK could explore a cooperative arrangement with European partners under the EU's proposed Cable Vessels Reserve Fleet, which envisions a shared pool of multi-purpose ships for emergency cable deployment and repair.

- **Support strategic stockpiling of cable repair parts with industry:** The UK should work with cable operators to ensure pre-positioned depots of critical components – such as repeaters, spare cable, and universal joints – at key maritime chokepoints such as the West Coast of Ireland or English Channel. This would reduce the mean time to repair in high-traffic or high-risk regions and improve resilience against both accidental damage and deliberate interference. The planned development of Subic Bay in the Philippines into a regional cable repair hub, supported by SubCom and reportedly backed by U.S. investment, provides a useful model.

- **Review and upgrade standards and regulations:** The UK should conduct a comprehensive review of its technical standards and regulatory frameworks for the construction, protection, and maintenance of undersea cables. This review should work with industry to assess current requirements for cable armouring and burial, as well as the effectiveness of warning systems, breakage detection, and the integration of new threat detection technologies. It should also examine licensing processes, including provisions for repair fleet availability, contingency planning, and the stockpiling of critical parts in the event of disruption.

Bibliography

Abke, Tom. 'Indo-Pacific Nations Bolstering Defense of Undersea Cables against Emerging Vulnerabilities'. *Indo-Pacific Defense FORUM* (blog), 18 September 2024. https://ipdefenseforum.com/2024/09/indo-pacific-nations-bolstering-defense-of-undersea-cables-against-emerging-vulnerabilities/.

Abramowicz, Victor. 'Russian Submarines: Threats and Opportunities for Britain – Britain's World'. *Council on Geostrategy* (blog), 26 September 2022. https://www.geostrategy.org.uk/britains-world/russia-submarines-and-aukus-threats-and-opportunities-for-britain/.

Alcatel Submarine Networks. 'Written Evidence Submitted by Alcatel Submarine Networks: Use of Fibre Sensing to Secure UK Subsea Infrastructure', 2025. https://committees.parliament.uk/writtenevidence/138747/html/.

Allison, George. 'MoD Tight-Lipped on Second Undersea Surveillance Ship', 3 February 2025. https://ukdefencejournal.org.uk/mod-tight-lipped-on-second-undersea-surveillance-ship/.

Antonov, Dmitry. '"Friends of Steel": Xi and Putin Pledge to Stand Together against US'. *Reuters*, 8 May 2025, sec. Europe. https://www.reuters.com/world/europe/putin-greets-chinas-xi-kremlin-2025-05-08/.

Chen, Stephen. 'China Unveils a Powerful Deep-Sea Cable Cutter That Could Reset the World Order'. South China Morning Post, 22 March 2025. https://www.scmp.com/news/china/science/article/3303246/china-unveils-powerful-deep-sea-cable-cutter-could-reset-world-order.

Cheung, Sunny, and Cheryl Yu. 'Creative Destruction: PRC Undersea Cable Technology', January 2025. https://jamestown.org/program/creative-destruction-prc-undersea-cable-technology/.

Clare, Mike. 'Submarine Cable Protection and the Environment'. The International Cable Protection Committee (ICPC), October 2024. https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_October_2024.pdf.

Crosslake Fibre UK Limited. 'Written Evidence Submitted by Crosslake Fibre UK Limited', 2025. https://committees.parliament.uk/writtenevidence/138661/html/.

Dotson, John. 'Strangers on a Seabed: Sino-Russian Collaboration on Undersea Cable Sabotage Operations'. *China Brief* 25, no. 3 (February 2025). https://jamestown.org/program/strangers-on-a-seabed-sino-russian-collaboration-on-undersea-cable-sabotage-operations/.

Essen, Hugo von. ‘Joint Military Exercises Signal Deepening Russia-China Strategic Alignment | Merics’, 7 May 2025. https://merics.org/en/comment/joint-military-exercises-signal-deepening-russia-china-strategic-alignment.

European Commission. ‘Joint Communication to Strengthen the Security and Resilience of Submarine Cables | Shaping Europe’s Digital Future’, 2025. https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables.

Freightlink. ‘Irish Sea Ferry Routes’, 2023. https://www.freightlink.co.uk/irish-sea-ferry-routes.

Hartmann, Jacques. ‘Written Evidence Submitted by Dr Jacques Hartmann, Professor in International Law and Human Rights, University of Dundee’, 2025. https://committees.parliament.uk/writtenevidence/139113/pdf/.

Hawkins, Amy. ‘China and Russia Pledge to Deepen Ties as They Criticise US on Victory Day’. *The Guardian*, 9 May 2025, sec. World news. https://www.theguardian.com/world/2025/may/09/china-russia-ties-criticise-us-victory-day.

Henrik Nilsson, Jeroen van Overloop, Raza Ali Mehdi, and Jonas Pålsson. ‘Transnational Maritime Spatial Planning in the North Sea: The Shipping Context’, 2018. https://northsearegion.eu/media/4566/032018_transnational-maritime-spatial-planning-in-the-north-sea-the-shipping-context.pdf.

Herlevi, April A. ‘China’s Strategic Space in the Digital Undersea - Mapping China’s Strategic Space’, 14 March 2024. https://strategicspace.nbr.org/chinas-strategic-space-in-the-digital-undersea/.

Hioe, Brian. ‘Another Severed Submarine Cable Raises Alarm in Taiwan’, 2025. https://thediplomat.com/2025/01/another-severed-submarine-cable-raises-alarm-in-taiwan/.

Hsu, Tso-Juei. ‘Taiwan’s FY2025 Defense Budget : An Overview of the New Naval Programs - Naval News’, 11 October 2024. https://www.navalnews.com/naval-news/2024/10/taiwans-fy2025-defense-budget-an-overview-of-the-new-naval-programs/.

Indeximate Ltd. ‘Written Evidence Submitted by Indeximate Ltd: Monitoring the Health and Security of Undersea Infrastructure’, 2025. https://committees.parliament.uk/writtenevidence/138675/html/.

International Cable Protection Committee. ‘Cableships of the World’, 2025. https://www.iscpc.org/information/cableships-of-the-world/.

Lii, Wen. ‘After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience’, April 2023.

https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/.

Lock, Charlotte. 'Geo Explainer: Where in the World Are the Busiest Shipping Lanes?' *Geographical* (blog), 10 October 2024. https://geographical.co.uk/news/geo-explainer-where-in-the-world-are-the-busiest-shipping-lanes.

McMahon, Liv. 'Meta Plans Globe-Spanning Sub-Sea Internet Cable'. BBC News, 17 February 2025. https://www.bbc.com/news/articles/ckgrgz8271go.

Ministry of Defence, Foreign, Commonwealth & Development Office, Keir Starmer, and John Healey. 'Joint Expeditionary Force Activates UK-Led Reaction System to Track Threats to Undersea Infrastructure and Monitor Russian Shadow Fleet'. GOV.UK, 2025. https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. 'Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War'. RAND Corporation, 27 June 2019. https://www.rand.org/pubs/research_reports/RR2942.html.

National Cyber Security Centre. 'NCSC Annual Review 2024', 2024. https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf.

NATO. 'NATO Launches "Baltic Sentry" to Increase Critical Infrastructure Security'. NATO, 2025. https://www.nato.int/cps/en/natohq/news_232122.htm.

NavyLookout. 'AI-Enabled Underwater Gliders Could Enhance Royal Navy ASW Capability | Navy Lookout', 13 May 2025. https://www.navylookout.com/ai-enabled-underwater-gliders-could-enhance-royal-navy-asw-capability/.

Offshore Energy. 'ASN, TE SubCom Get Telefónica Maintenance Contract Extension'. *Offshore Energy* (blog), 26 May 2016. https://www.offshore-energy.biz/asn-te-subcom-get-telefonica-maintenance-contract-extension/.

Pancevski, Bojan. 'Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables'. WSJ, 29 November 2024. https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1.

Panella, Chris. 'A British Submarine Secretly Tracking a Russian Spy Ship Hanging around Undersea Cables Surfaced Close to It to Send a Message, UK Says'. Business Insider, 2025. https://www.businessinsider.com/uk-sub-secretly-watched-russian-spy-ship-near-undersea-cables-2025-1.

Park, William. ‘The Deep-Sea “emergency Service” That Keeps the Internet Running’, October 2024. https://www.bbc.com/future/article/20241014-the-deep-sea-emergency-service-that-keeps-the-internet-running.

Pedrozo, Raul (Pete). ‘Safeguarding Submarine Cables and Pipelines in Times of Peace and War’. Stockton Center for International Law, 2025. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3099&context=ils.

Reuters. ‘EU to Spend Nearly a Billion Euros to Protect Undersea Cables’. *Reuters*, 21 February 2025, sec. Europe. https://www.reuters.com/world/europe/eu-will-propose-establishing-fleet-vessels-emergency-undersea-cable-repairs-2025-02-21/.

Ripley Tools. ‘Taking a Closer Look at the Anatomy of a Fiber Optic Cable’, 25 October 2022. https://www.ripley-tools.com/taking-a-closer-look-at-the-anatomy-of-a-fiber-optic-cable/.

Roth, Andrew, and Vincent Ni. ‘Xi and Putin Urge Nato to Rule out Expansion as Ukraine Tensions Rise’. *The Guardian*, 4 February 2022, sec. World news. https://www.theguardian.com/world/2022/feb/04/xi-jinping-meets-vladimir-putin-china-russia-tensions-grow-west.

Ryzhenko, Andrii. ‘Russia Looks to Target Achilles’ Heel of Western Economies on Ocean Floor | RealClearDefense’, 19 September 2024. https://www.realcleardefense.com/articles/2024/09/19/russia_looks_to_target_achilles_heel_of_western_economies_on_ocean_floor_1059375.html.

Sabanadze, Natalie, Abigaël Vasselier, and Gunnar Wiegand. ‘China-Russia Alignment: A Threat to Europe’s Security | Merics’, 26 June 2024. https://merics.org/en/report/china-russia-alignment-threat-europes-security.

Saxena, Anushka. ‘China’s Show of Force With Belarus Amid NATO Concerns’, 17 July 2024. https://thediplomat.com/2024/07/chinas-show-of-force-with-belarus-amid-nato-concerns/.

Sher, Nathaniel. ‘Behind the Scenes: China’s Increasing Role in Russia’s Defense Industry’. Carnegie Endowment for International Peace, May 2024. https://carnegieendowment.org/russia-eurasia/politika/2024/05/behind-the-scenes-chinas-increasing-role-in-russias-defense-industry?lang=en.

Soong, Claus. ‘China-Russia Alignment – a Shared Vision, without Fully Seeing Eye to Eye’, 7 May 2025. https://merics.org/en/comment/china-russia-alignment-shared-vision-without-fully-seeing-eye-eye.

Spinergie. ‘How offshore cable repair operations impact the market’, 2024. https://www.spinergie.com/blog/offshore-cable-repair-market-impact.

Submarine Telecoms Forum, Inc. ‘Industry Report 2021/2022’, 2021. https://cnetworks.info/wp-content/uploads/2021/11/Submarine-Telecoms-Industry-Report-Issue-10.pdf.

———. ‘SubTel Forum Submarine Telecoms Industry Report’. *SubTel Forum* (blog), 2023. https://subtelforum.com/industry-report/.

Systematic. ‘SitaWare Delivers Situational Awareness of UK Waters’, no date. https://systematic.com/int/industries/defence/news-knowledge/cases/sitaware-delivers-maritime-situational-awareness-of-uk-waters/?utm_source=chatgpt.com.

Taipei Times. ‘Coast Guard Drove Away 567 Chinese Boats in 6 Months’, 5 July 2024. https://www.taipeitimes.com/News/taiwan/archives/2024/07/05/2003820369.

TeleGeography. ‘Submarine Cable Map’, 2025. https://www.submarinecablemap.com/.

The Baltic Times. ‘Estonia Tightening Criminal Law to Protect Underwater Infrastructure’, 2025. https://www.baltictimes.com/estonia_tightening_criminal_law_to_protect_underwater_infrastructure/.

The Maritime Executive. ‘Chinese Ship Suspected of Cable Sabotage May Have Had Two AIS Devices’, January 2025. https://maritime-executive.com/article/chinese-ship-suspected-of-cable-sabotage-may-have-had-two-ais-devices.

UK Government. ‘Written Evidence Submitted by HM Government to the Questions Posed in the Joint Committee for National Security Strategy’s Call for Evidence on Undersea Cables.’, 2025. https://committees.parliament.uk/writtenevidence/138673/pdf/.

UK Space Agency. ‘UK Satellites to Boost Maritime Security on Track for 2025 Launch’. GOV.UK, 23 October 2024. https://www.gov.uk/government/news/uk-satellites-to-boost-maritime-security-on-track-for-2025-launch.

United Nations. ‘United Nations Convention on the Law of the Sea’, 1994. https://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm.

Wall, Colin, and Pierre Morcos. ‘Invisible and Vital: Undersea Cables and Transatlantic Security’. *Centre for Strategic & International Studies*, 6 November 2021. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security.

Webster, Katie. ‘ACMA 2017 Agreement Extended to the End of 2025 With Suppliers Global Marine and Orange Marine’. *Global Marine* (blog), 25 November 2020. https://globalmarine.co.uk/acma-2017-agreement-extended-to-the-end-of-2025-with-suppliers-global-marine-and-orange-marine/.

Wei-li, Fang, and Jonathan Chin. ‘China Ship Used Taiwan Ports for Months - Taipei Times’, 2 March 2025. https://www.taipeitimes.com/News/front/archives/2025/03/02/2003832732.

Wickham, Alex. ‘UK Cyber Security Chief Names China as Dominant Hacking Threat’. *Bloomberg.Com*, 7 May 2025. https://www.bloomberg.com/news/articles/2025-05-07/uk-cyber-security-chief-names-china-as-dominant-hacking-threat.

Windward. ‘Illuminating Russia’s Shadow Fleet’, 2024. https://windward.ai/knowledge-base/illuminating-russias-shadow-fleet/.

Wodecki, Ben. ‘Sweden Finds No Proof Chinese Ship Cut Baltic Cables on Purpose’. Capacity Media, 15 April 2025. https://www.capacitymedia.com/article/sweden-finds-no-proof-chinese-ship-cut-baltic-cables-on-purpose.

Cover image: U.S. Navy photo by Chief Equipment Operator Adam Winters[69]

[69] https://www.flickr.com/photos/compacflt/9510971787