Undersea Cables

Evidence submission by RAND Europe

Henri van Soest, Harper Fine, James Black, Lucia Retter, Zsofia Wolford

CT-A4112-1

Prepared for the Joint Committee on National Security Strategy

For more information on this publication, visit www.rand.org/t/CTA4112-1

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

© 2025 RAND Corporation

RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights
This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorised posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

Undersea Cables

Written evidence submitted by Henri van Soest,
Harper Fine, James Black, Lucia Retter, Zsofia Wolford[1]
RAND Europe[2]

Prepared for the Joint Committee on National Security Strategy

6 March 2025

This document provides RAND Europe's submission of evidence in relation to the Joint Committee on National Security Strategy's Call for Evidence on Undersea Cables. This document is structured to reflect the questions in the Committee's call for evidence.[3]

RAND Europe is the European arm of RAND, a not-for-profit research institute with a mission to improve policymaking through robust research and analysis. RAND combines academic rigour with a targeted consultancy approach and is committed to the public interest and to making our work accessible. RAND has 75 years of experience helping governments and militaries navigate complex choices and prepare robust strategic approaches in a range of sector and policy areas.

This document draws upon this extensive body of previous RAND research including previous work for the UK Government, NATO and others on critical undersea infrastructure.

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND Europe or any of the sponsors of its research.

[2] RAND Europe is a research organisation that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND Europe is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behaviour. RAND Europe subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND Europe routinely draw on relevant research conducted in the organisation.

[3] UK Parliament (2025)

1. Summary

Q1: How might the UK's reliance on undersea cables evolve over the next 10-15 years?

- Undersea telecommunications cables carry more than 97 percent of the world's telecommunications. They also play a vital role in connecting global financial markets, transmitting £8 trillion in financial transactions every day.
- The UK's critical undersea infrastructure (CUI) is poised for significant growth and transformation in the coming decades. While an increasing number of undersea cables may improve resilience, growing digitisation will make society even more dependent on this CUI.
- Alternative approaches, like satellite communications, may offer some potential diversification but these technologies cannot match the high bandwidth provided by undersea cable infrastructures.

Q2: Who are the main threat actors to undersea cable infrastructure and what are their capabilities?

- Overall, deliberate disruptions to CUI remain relatively rare, and the most common causes of disruption remain accidents and negligence.
- For around 20 per cent of known undersea disruptions, a definitive cause is never found. The difficulty of identifying, evidencing, and attributing the cause of a given disruption makes the undersea domain well-suited to so-called 'hybrid', 'grey zone' or 'sub-threshold' tactics.
- There are a limited number of highly capable state actors with the capacity to cause deliberate disruptions to CUI. In the UK context, Russia and China are the most important. Russia has specialist naval and intelligence ships, as well as impressive submarine capabilities; the UK's competitors also leverage exploit a 'ghost fleet' of commercial vessels for deniable attacks on CUI. Chinese companies have, in turn, invested heavily in European undersea infrastructure companies, posing potential risks for security.
- The proliferation and falling costs of technologies, such as uncrewed underwater vehicles (UUVs) could enable disruption by less capable state actors and by non-state actors, such as criminals, terrorists, hackers, protest groups and others.

Q3: What developments are expected in subsea technologies over the next 10 years?

- The ongoing digital revolution is expected to expand the digital economy and drive a continued rapid growth in internet traffic, both in Europe and globally. This will lead to a significant growth in undersea cable infrastructure. Likewise, there will be substantial growth in other types of CUI,

namely electricity interconnectors (e.g., to link the UK to offshore wind farms, continental European electricity grids or North African solar power projects) and oil and gas pipelines. Collectively, this will drive greater investment in CUI – and potential hostile interest in disrupting it.

- The ongoing digitalisation of CUI is a double-edged sword when it comes to managing security risks. For example, UUVs can be used for offensive purposes, but can also be used to monitor, maintain and protect CUI. Automation offers efficiencies but also brings new cyber vulnerabilities.
- The UK is well-positioned to play a key role in the further development of subsea technology. Given its current role as a hub for transatlantic cables, the North Sea oil and gas production, and continuing investment in offshore wind, the UK already has a lot of experience in subsea engineering that can be repurposed. The UK also has a strong research ecosystem, and it is a leader in key enabling technologies, such as AI. Finally, the UK plays a key role in many existing cable protection initiatives, such as the NATO Maritime Centre for the Security of Critical Infrastructure at MARCOM in Northwood or the work of the Joint Expeditionary Force (JEF), enabling the rapid deployment of advanced protection measures.

Q4: How resilient are the UK public and private sectors likely to be in the event of major disruption?

- A large, coordinated disruption could have immediate effects on finance, communications, government functions, and payments. Strategic and sustained disruptions could impact entire systems and lead to spiralling costs of disruption, which would impact most sectors of the wider economy and disrupt essential services like banking, energy, defence, food supply, and healthcare.
- The nature, impact and duration of any disruption is influenced by many factors, based on the affected systems' built-in resilience and redundancy (or lack thereof), and the speed and effectiveness of any response from the public and private sector actors involved in different aspects of CUI.

Q5: How effective are the deterrents against the targeting of our undersea cables?

- Deterrence has an essential role to play in dissuading hostile actors from interfering with CUI. Protecting CUI amidst escalating threats entails the need for a mix of both 'deterrence by denial' and 'deterrence by punishment', with both approaches serving to increase the political, financial and operational costs of adversaries attacking CUI.
- The UK has relevant maritime security capabilities, such as surveillance aircraft, nuclear attack submarines, and Multi-Role Ocean Surveillance (MROS) ships. RFA Proteus, the first Multi-Role Ocean Surveillance (MROS) ship has however faced delays in undertaking its core tasks due to conversion and staffing issues.
- The JEF, in which the UK plays a leading role, has been an effective mechanism for deepening military ties and improving interoperability between its members. It has played a pivotal role in integrating Sweden and Finland into the wider European military architecture, prior to these countries joining NATO in 2024. It has also activated Response Options to conduct joint patrols of CUI in response to recent attacks, dubbed NORDIC WARDEN.

- NATO has established an operationally focused Maritime Centre for the Security of Critical Undersea Infrastructure at MARCOM in Northwood, in the UK. This centre focuses on preparing for, deterring, and defending against hybrid attacks and improving situational awareness and response capabilities. In a sign of the continuing escalation of threats against CUI in the Baltic Sea region especially, in January 2025 NATO's new Secretary-General, Mark Rutte, announced a new joint military effort, BALTIC SENTRY.

Q6: How well is policy and co-ordination working across Whitehall departments, law enforcement and private sector actors? Are any changes needed?

- Responsibilities and policy levers for CUI are spread across multiple departments, presenting co-ordination challenges. The Department for Science, Innovation and Technology (DSIT) is the policy lead for undersea cables, while the Department for Energy Security and Net Zero (DESNZ) is responsible for electricity interconnectors and oil and gas pipelines. There are also issue-specific roles for agencies such as the Maritime and Coastguard Agency (MCA), part of the Department for Transport (DfT), or for law enforcement, intelligence agencies and the National Cyber Security Centre (NCSC). In practice, the Royal Navy and consequently the Ministry of Defence (MOD) have the only military assets to defend or deter attacks on CUI, but they lack corresponding dedicated funding for this task.

- Because so many players are involved in the protection of undersea infrastructure, sharing information is a vital enabler of any security, resilience or deterrence efforts. Governments and the private sector should find mutually agreeable ways to share information to maximise effectiveness in protecting CUI. While this is challenging, the importance of doing so is paramount given the scale and scope of CUI.

- Given their cross-border nature, there is also a need for cooperation with international allies and partners – hence the importance of bilateral cooperation (e.g., with France, Belgium, Netherlands, Norway, Ireland) and a strong UK input to the JEF, NATO and other multilateral initiatives.

Q7: In the context of limited resources, what is the appropriate balance to strike between enhancing domestic resilience on the one hand, and improving detection and interdiction on the other?

- Fixing crewed naval assets, already in short supply, on lengthy patrols of CUI implies opportunity costs that only serve adversaries' interests: enabling hostile actors to tie down high-value assets from NATO navies on CUI-related taskings with relatively little effort. As such, more sustainable long-term solutions are required, including using assets with less relevance to warfighting and exploiting advances in uncrewed systems, AI, sensors and other technologies.

- The private sector should bear greater responsibility for the protection of CUI and adopt a duty of care (whether motivated by regulation, insurance requirements, or other means). The operators of critical undersea infrastructure should become the first line of defence against hybrid warfare. When planning and constructing new infrastructure, they should make this infrastructure more resilient and secure by design.

- While this evidence submission focuses on undersea telecommunications cables, it is important to note that the landscape of CUI covers several other types of infrastructure, including undersea power cables and undersea oil and gas pipelines. These cannot be addressed in isolation; a comprehensive approach to CUI protection is essential.

2. How might the UK's reliance on undersea cables evolve in the next 10-15 years?

2.1. What are the key vulnerabilities at the moment and how might these change? (Including both undersea infrastructure and onshore cable landing stations)

Undersea communication cables are fibre-optic cables used to transfer information over long distances, connecting countries and continents. Despite advances in alternative technologies such as satellite communications, submarine cables still carry more than 97 percent of the world's telecommunications.[4] These cables also play a vital role in connecting global financial markets, transmitting £8 trillion in financial transactions every day.[5] The UK is heavily reliant on undersea cables, and as sectors of the UK economy become increasingly digitised, the number of undersea cables serving the UK and the volume of data they carry is expected to grow significantly.

Undersea infrastructure has distinctive characteristics that create specific vulnerabilities. Many assets are poorly protected physically, often being laid in a shallow ditch or even just on the seabed itself. Their primary defence is their remote location, rather than any physical hardening against attack or any routine surveillance and protection by maritime assets. The large scale and widespread geographic distribution of CUI makes continuous monitoring and physical presence across the whole network both impractical and cost-prohibitive, particularly when relying on crewed naval assets.[6]

Moreover, the many public and private stakeholders involved in commissioning, building, operating, maintaining, and regulating CUI complicate the allocation of responsibilities, costs, and risks. Because CUI often links different countries, and may pass through third countries, different parts of a single CUI may be covered by multiple jurisdictions.[7]

Technological progress may help address vulnerabilities but may also lead to the development of new ones. For example, uncrewed underwater vehicles (UUVs) and the deployment of advanced metering systems can enhance the protection and monitoring of assets without the need for human presence. However, UUVs can also be used by hostile actors for offensive purposes, including reconnaissance or sabotage of CUI assets,

[4] Sunak (2017)

[5] Sunak (2017)

[6] van Soest et al. (Forthcoming)

[7] van Soest et al. (Forthcoming)

while the use of advanced metering can introduce new cyber vulnerabilities. Box 2.1 outlines major vulnerabilities facing CUI.

Box 2.1 Key vulnerabilities of undersea infrastructure

- The vast extent of undersea infrastructure, making continuous monitoring or protection (e.g., by naval assets) prohibitively costly
- Clustering of crucial hubs and nodes in certain waters, as well as proximate cable landing points, which may make disruptions to these areas particularly damaging
- Substantial publicly accessible data on the location and characteristics of undersea infrastructure, which cannot be relocated and thus is easily targeted
- Additional risks associated with cable landing sites on the shoreline, which can be disrupted by a wider range of capabilities
- A large number of stakeholders across both the public and private sectors (e.g., with multiple government departments and companies involved), which can hinder effective coordination
- A lack of standardisation across infrastructure owned by different companies or countries
- Increasing automation and digitisation, which brings efficiency but also new dependencies
- Technological innovation improving monitoring and defence, but also enhancing attack capabilities
- Legal ambiguities in governance, particularly for infrastructure located beyond 12 nautical miles territorial waters of sovereign countries
- Finite capacity of the specialist ships and equipment required to inspect, repair and replace damaged cables or pipeline, presenting a challenge if multiple infrastructures are damaged at once
- The growing dependence on CUI, which makes it a desirable target for a range of threat actors both in the grey zone between competition and conflict, and in times of open war (e.g., against NATO)

Source: Sunak (2017); Runde et al. (2024); Bueger et al. (2022); Bekkers et al. (2021); van Soest and Fine (2024); Paik and Counter (2024). Box taken from van Soest et al. (Forthcoming).

2.2. How does this compare to the situation in other countries (particularly island states)?

As an island nation, the UK relies heavily on CUI for global economic connectivity, international communications, and access to vital energy inputs such as natural gas and electricity. However, the UK is not unique in its dependence on CUI. While coastal states are generally more directly dependent on subsea infrastructure, even landlocked countries rely on these networks for global connectivity. For example, about two-thirds of the cables ensuring the EU's connection to the global internet are submarine cables.[8]

Taiwan is a notable parallel to the UK in terms of undersea infrastructure. It is the landing point for 14 international subsea cables, in addition to 10 cables connecting the main island of Taiwan to smaller neighbouring islands. Taiwan also has a growing offshore wind sector. For example, the Fengmiao 1 offshore wind park will be connected to the island of Taiwan through two 45 kilometre cables.[9] To serve this industry, Taiwan has announced plans for its first subsea power cable factory, which is due to be completed by

[8] Besch and Brown (2024)

[9] Memija (2024)

2027.[10] Although Taiwan imports all its oil and almost all of its natural gas via shipping, it has a limited number of subsea gas pipelines that connect different terminals in the island's gas grid.[11] Unlike the UK, however, the region around Taiwan is prone to natural disasters, such as earthquakes and tsunamis, which can damage undersea infrastructure. Taiwan has also faced sabotage incidents, such as a January 2025 incident affecting a subsea cable connecting Taiwan and the Matsu Islands.[12] Like Western countries, Taiwan has been working on improving its resilience to disruptions to CUI, such as developing multi-level backup communications systems based on different technologies.[13]

Crucially, the UK's adversaries and competitors are not equally reliant on undersea cables, as they are primarily continental powers with extensive land-based communication networks. This represents a particular challenge for Europe and NATO, though any major and sustained disruptions in that region could also have consequences for the global economy and markets more broadly.

2.3. Are there any long-term alternatives to undersea cable infrastructure?

There are currently no clear alternatives, even in the long-term, to undersea cable infrastructures. While satellite communications may offer an alternative for the most critical applications, they are unlikely to provide sufficient bandwidth to offer a meaningful alternative to subsea telecommunications cables. Furthermore, reliance on space-based systems brings its own set of risks and vulnerabilities, whether political, cyber or military in nature.[14]

[10] Buljan (2023)

[11] Taiwan Ministry of Economic Affairs (2025)

[12] Thompson and Ming-yan (2025)

[13] Bilinski (2025)

[14] Gerstein and Leidy (2025)

3. Who are the main threat actors to undersea cable infrastructure and what are their capabilities?

A series of high-profile incidents involving CUI disruption has highlighted its vulnerability, prompting discussions about its security and the potential for exploitation in grey zone competition or open conflict. Nonetheless, open-source information indicates that deliberate disruptions remain comparatively rare.

CUI risks are typically broken down into: (1) accidents and negligence; (2) natural hazards; (3) state action; and (4) non-state action.[15] Accidents and negligence are still the most common causes of disruption, often stemming from issues during the manufacturing and installation process or unintentional external interference, such as a ship dragging an anchor. Fishing-related damage alone is estimated to account for over 40 per cent of known disruptions. The second leading cause of disruption involves natural factors, including underwater landslides, wave action in extreme storms, or soil liquefaction, together accounting for 15 percent of disruptions.[16]

While deliberate action by state or non-state actors has not historically been a major cause of disruption, it poses a growing threat—heightened since Russia's full-scale invasion of Ukraine in 2022—and the consequences of a major, coordinated assault on CUI could be devastating.

A small number of state militaries and intelligence services are known to possess capabilities to interfere with CUI, with Russia and China constituting the primary threats to Europe and NATO. In addition to physical attacks, undersea telecommunications cables can also be exploited for espionage and information gathering purposes. They may provide adversaries with opportunities to intercept, copy and steal data, including sensitive diplomatic and even military communications that pass through some of the cables. Cable tapping can occur through various methods, such as via the insertion of backdoors during manufacturing of components in the supply chain, by targeting landing stations and onshore facilities that link cables to networks on land, or by tapping cables out at sea. Table 3.1 outlines the various forms of military threats to CUI.

[15] Bekkers et al. (2021)

[16] Sunak (2017)

Table 3.1 Types of military threats with relevance for undersea infrastructure

Type of threat	Description
Physical attacks	Military operations targeting maritime functions, vessels and structures, military or otherwise. This could include using submarines or UUVs to cut undersea cables, damage pipelines, and destroy underwater monitoring systems.
Cyber and electromagnetic activities	Military operations to destroy, degrade, jam, spoof or take control of information and communications technology systems of vessels or maritime structures, military or otherwise. Cyber-attacks on CUI could include the injection of malware, electromagnetic pulse attacks, and electronic jamming to telecommunications cables.
Anti-access, area denial	Military operations to disrupt or hinder access to and use of the sea, by using physical barriers, mines, or other deterrents. This could include preventing access to key underwater areas, which would limit undersea surveillance, as well as hinder the repair and maintenance of CUI.
Espionage	Military operations to gather intelligence, for example by tapping undersea communication cables to gain access to data transmissions or deploying uncrewed sensor platforms at sea. These operations could compromise secure communications and reveal strategic information.
Raids and landings	Military operations to access the land from the sea, ranging from small-scale and covert deliverance and extraction of units to larger amphibious operations. These attacks could target critical infrastructures, including cable landing sites.

Source: Bekkers et al. (2021). Table taken from van Soest et al. (Forthcoming).

About 20 per cent of undersea disruptions lack a definitively identified cause. The challenge of identifying, evidencing, and attributing the cause of a given disruption makes the undersea domain well-suited to so-called 'hybrid', 'grey zone' or 'sub-threshold' tactics, where hostile state action is coupled with secrecy and plausible deniability. The ambiguity surrounding these actions allows perpetrators to push boundaries of permissible behaviour while hindering efforts to mobilise political, legal, or military responses. The high value of the services provided by CUI and the corresponding high cost and impact of disruption means that CUI are an attractive target for grey-zone activities, supporting wider efforts to disrupt or influence the information environment or to undermine connectivity within Europe or NATO. Table 3.2 summarises the several types of potential grey-zone activities of relevance to CUI.

Table 3.2 Types of grey-zone threats with relevance to undersea infrastructure

Type of threat	Description
Sabotage	Covert, deliberate damage to maritime vessels or infrastructure for strategic advantage in peacetime.
Cyber operations	Actions aimed at covertly monitoring or interfering with information and communications technology (ICT) systems of maritime structures.
Espionage	Military operations to gather intelligence, for example by tapping communication cables or deploying uncrewed sensor platforms at sea.
Incursions	Grey-zone actions, often by military vessels, that violate a coastal state's sovereignty, either openly or covertly, to probe defences or to 'show the flag'. This could extend to essential undersea systems, particularly those within the 12 nautical mile territorial waters of sovereign countries.

Source: Bekkers et al. (2021). Table taken from van Soest et al. (Forthcoming).

Historically, the remote environment of CUI offered protection, and only a small number of highly capable nation states had the capabilities to interfere with CUI. However, technological change has meant that offensive technologies are now also becoming available to less capable state actors and non-state actors. In addition, cyberattacks are becoming increasingly accessible and can be effective and, in the case of ransomware, lucrative ways for non-state actors to target and disrupt CUI and related services. These possibilities for financial and reputational gain thus further increase the number of potential threat actors and the complexity of the threat landscape. For example, there are concerns that Houthi militants in Yemen may target subsea cables in the Red Sea.[17] They are known to possess several underwater capabilities, such as limpet mines and guided torpedoes, and militants have reportedly undertaken combat diver training in the Red Sea.[18]

[17] Johnson (2024)

[18] Nadimi and Knights (2018); Nadimi (2023)

4. What developments are expected in subsea technologies over the next 10 years?

CUI is set for significant growth and transformation in the coming decades, which is likely to offer many benefits but also create new dependencies and risk. The digital revolution is expected to lead to an expansion of the digital economy and drive a continued rapid growth in Internet traffic, both in Europe and globally. Although satellite communications may become more prevalent and offer an alternative to undersea cables for some use cases, they will not be able to provide a full replacement to the high-capacity and low latency communications that undersea telecommunications cables offer.

To manage the surge in internet traffic, large amounts of additional undersea telecommunications cables are being planned and constructed to augment the current network. While the creation of more undersea assets will help to improve redundancy, greater reliance on this infrastructure will create a higher-impact, higher-value target for threat actors. Furthermore, advances in automation could limit human oversight and increase dependency on remote network management systems, making CUI more vulnerable to cyber-attacks.[19]

Simultaneously, the urgent need to combat climate change is accelerating the deployment of renewable energy sources and the associated electrification of industry, transportation, and other economic activities. This will lead to growth in the number of undersea electricity cables. While the depletion of reserves and climate concerns may result in the decommissioning of much oil and gas infrastructure, some existing pipelines could be repurposed for hydrogen transport and carbon capture, utilisation, and storage initiatives.[20]

Key enabling technologies are also evolving quickly. Control systems are increasingly digitised, remote sensing equipment is being widely deployed across CUI, uncrewed vehicles (such as UUVs) are advancing rapidly, and developments in artificial intelligence and data analytics enable more granular monitoring and control of CUI.[21]

4.1. Do these favour aggressors or defenders?

New technologies can be deployed for both offensive and defensive uses. For instance, while UUVs help secure undersea assets, they could also be employed in sabotage missions. Whether a particular technology

[19] van Soest et al. (Forthcoming)

[20] van Soest et al. (Forthcoming)

[21] van Soest et al. (Forthcoming)

benefits attackers or defenders depends heavily on the context of its use. As such, the key differentiating factor is the 'intent' with which the technology is used.

Advances in undersea technology may lower barriers to entry for actors wishing to attack undersea infrastructure, potentially leading to an increase in the number of threat actors. Greater affordability and accessibility could open the door to a proliferation of the use of drone technology by hostile states, criminals, terrorists, hackers, protest groups and others, and enable new forms of disruption while simultaneously complicating the task of attribution.[22] On the other hand, disruption of subsea assets through grey zone activities, such as anchor dragging, is already possible. While less sophisticated actors can already conduct simple sabotage operations on subsea infrastructure, technological developments may enable these actors to conduct more complex operations.

One of the key issues for defenders is the sheer size and geographic disparity of subsea infrastructure. Technological developments could be very helpful in overcoming these challenges. Electronic monitoring systems can improve the physical and data security of subsea cables by identifying changes or irregularities in the seabed environment and notifying operators. Additionally, electronic protection, such as end-to-end encryption, helps mitigate the risks of surveillance, tapping, and espionage.[23] However, an increasing reliance on internet-connected remote management systems may also introduce new cybersecurity risks.

4.2. How well positioned is the UK to take advantage?

The UK's location in the North Atlantic and the North Sea make it a natural hub for subsea technology. The UK is a hub for transatlantic cables linking the US and continental Europe. The North Sea is a critical area for oil and gas production and offshore wind energy, which require advanced subsea technology. The UK also has large ports to handle maintenance, logistics, and deployment of subsea technology.

The UK has extensive experience in offshore oil and gas extraction in the North Sea. This experience provides a solid foundation for future subsea developments, as many of the technologies and techniques used in offshore oil and gas exploration and production can be adapted for new subsea applications, such as offshore renewable energy generation and subsea carbon capture. The UK is also a global leader in offshore wind energy. As offshore wind farms grow in scale and complexity, the need for advanced subsea cables, turbines, and infrastructure will grow, driving demand for innovative subsea solutions.

The UK also has a strong research and development ecosystem. It is home to several companies and research institutions that specialise in UUVs, uncrewed surface vehicles (USVs), and uncrewed aerial vehicles (UAVs). These technologies are critical for offshore exploration, maintenance, and environmental monitoring. The UK is also a leader in digital technology, including artificial intelligence (AI), machine learning, and big data analytics. These technologies are increasingly being applied in subsea operations, particularly in predictive maintenance and real-time monitoring of offshore systems.

[22] van Soest et al. (Forthcoming)

[23] Runde et al. (2024)

The UK plays a prominent role in various multinational CUI-monitoring initiatives. It hosts NATO's Maritime Centre for the Security of Critical Infrastructure at MARCOM in Northwood.[24] The UK is also the lead nation in the Joint Expeditionary Force, steering both strategic oversight and command. These multilateral efforts are discussed in more detail in Section 6.

[24] NATO (2024b)

5. How resilient are the UK public and private sectors likely to be in the event of major disruption?

5.1. Which sectors would be most affected?

Although isolated disruptions may cause only limited harm, coordinated attacks on critical nodes could reverberate across many industries. A large disruption could instantly affect the finance sector, communications, public administration, and payments systems. A well-planned, sustained disruption might affect entire markets, leading to rapidly escalating economic costs, which in turn would impact energy, financial services, defence, food supply, and healthcare. UK Government should conduct detailed risk assessments of CUI as part of national preparedness efforts. Detailed information on the impacts of CUI disruption on specific economic sectors should not be kept in the public domain.

5.2. What would be the immediate and long-term implications?

Disruptions to CUI can trigger complex impacts both in the short- and long-term, considering the interconnectedness of broader economic, governmental, and social systems with CUI. Immediate impacts of a major disruption could include the loss of internet connectivity, disruptions to banking systems, global trade, communication systems, and the increased vulnerability of national infrastructures. Long-term implications could include increased operational costs in countries reliant on vulnerable CUI. The broader economic cost of disruption depends on a number of factors, such as the location, the redundancy of the infrastructure, and the length of disruption. Table 5.1 below demonstrates the estimated total cost of disruptions for different infrastructure types.

Table 5.1: Total cost of disruption

Infrastructure type	Rough-order-of-magnitude (ROM) cost of disruption per day to a single piece if infrastructure	Average repair time	Total ROM cost of disruption
Subsea telecommunications cable	€24 million/day	7-24 days	€168 - 576 million
Electricity interconnectors	€12 million/day	40-60 days	€480 - 720 million
Gas pipelines	€75 million/day	5-9 months	€11.3 - 20.3 billion
Oil pipelines	€36 million/day	5-9 months	€5.4 - 9.7 billion

Source: RAND Europe analysis, drawing on publicly available data and costs. Table taken from van Soest et al. (Forthcoming).

5.3. What might be the constraints on restoring connectivity swiftly?

The speed and effectiveness of any response from both the public and private sector actors involved in managing different aspects of CUI depend on several factors, such as:

- the remoteness of the infrastructure,
- the weather,
- jurisdictional issues that could hinder timely responses
- investigation of the damage,
- potential simultaneous incidents,
- and limited availability of geographical distance of repair capacities, such as specialised personnel, vessels, etc.[25]

Table 5.2 details the nature of repairs and levels of resilience and redundancy typically found across undersea telecommunications cables, electricity cables, and oil and gas pipelines.

[25] van Soest et al. (2025).

Table 5.2 Resilience and redundancy of undersea infrastructure

Infrastructure type	Average repair time	System resilience and redundancy	Overview of strengths and vulnerabilities
Telecommunications cables	7-24 days	High, because of the large number of undersea cables and shorter repair times	Owners of undersea cables pay into a cooperative that has a repair vessel on standby to conduct repairs at short notice, using stored supplies. Repair vessels are primarily operated on commercial terms rather than being under the direct control of a potentially impacted government. Amidst concurrent disruptions, variations in cable ownership coupled with finite repair vessels could lead to coordination challenges.
Electricity cables	40-60 days	Medium, because of the smaller number of cables and longer repair times	The electricity grid is designed to accommodate an outage in any two nodes without disruptions to customers. However, cables and interconnectors do not yet benefit from a mature maintenance ecosystem. Given this lack of standardisation, individual owners of undersea electricity cables rely on their own contingency plans and their own stock of spare cables and joints. Electricity cables are often equipped with fibreoptic monitoring sensors that enable quick localisation of disruptions. Despite the potential for quick problem identification, however, repairs remain complex and time-consuming.
Oil and gas pipelines	5-9 months	Low, because of the lack of pipeline redundancy and longer repair times	Oil and gas pipelines are built using thick steel and are sometimes encased in concrete, enhancing their physical resilience. The oil and gas industries have a systematic focus on preventive maintenance. Yet, oil and gas pipelines typically have the lowest level of redundancy, and the disruption of a pipeline connecting an oil or gas field to the mainland could result in the entire field being shut down. If a pipeline's damage is limited, corrective maintenance will be carried out. However, if the damage is extensive, a full repair may be infeasible due to the complexity, expensiveness, and time needed. There is also the potential for significant environmental or climate damage as a result of any oil or gas leak.

Source: McLachlan (2018); Fisher (2022); Detecon (2013); Sechrist (2010). Table taken from van Soest et al. (Forthcoming).

6. How effective are the deterrents against the targeting of our undersea cables?

Deterrence is essential to discourage hostile actors from interfering with CUI. One key dimension is addressing the ambiguity that emboldens hybrid actions—for instance, by forcibly inspecting suspect vessels or cracking down on Russia's 'shadow fleet' involved in sanctions evasion.[26] Protecting CUI amidst escalating threats needs to include both 'deterrence by denial' and 'deterrence by punishment', and impose political, financial and operational costs to adversaries attacking CUI to discourage such attacks. Any effort to deter must be perceived as credible by hostile actors, necessitating strong political resolve to act in addition to the capabilities to do so. Deterrence, for instance, could include signalling such as when the Royal Navy deliberately surfaced an Astute-class nuclear attack submarine close to the Russian intelligence-gathering ship Yantar as an act of deterrence after it was found to be lingering over oil and gas pipelines and undersea cables in the Irish Sea.[27]

6.1. Maritime security capabilities

The UK has a number of relevant maritime security capabilities, including surveillance aircrafts and a fleet of nuclear attack submarines. The most important of these is RFA Proteus, the first Multi-Role Ocean Surveillance ship dedicated to protecting seabed telecommunications cables and oil/gas pipeline.[28] While it has formally been operational since 2023, it is not expected to start CUI patrols in 2025 due to conversion and staffing issues.[29]

In addition, the UK has had particular success through the Joint Expeditionary Force. The JEF has ten member countries (Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, the Netherlands, Norway, Sweden, and the UK) with the capability to deploy over 10,000 personnel for crisis response, deterrence and defence purposes. Maritime security is a critical aspect of the UK-led JEF, with member states holding regular joint naval exercises, and investing in underwater surveillance of CUI, information and intelligence sharing. The JEF also has rapid incident response protocols in place for both damages caused by natural causes and for deliberate sabotage.[30]

[26] van Soest (2025)

[27] Navy Lookout (2025)

[28] Allison (2023)

[29] Navy Lookout (2024)

[30] Joint Expeditionary Force (2024a)

The protection of CUI is a priority for the JEF. For instance, in 2023, its Member States organised Exercise AURORA that featured a multinational table-top exercise on threats to CUI, facilitating multi-state cooperation and garnering international attention to the growing risks to undersea assets.[31]

The JEF also activated Response Option NORDIC WARDEN in response to threats against CUI in the North, Norwegian and Baltic Seas. This helped to bring the naval and air capabilities of members together to monitor shipping activity near vital undersea energy and communications infrastructure, and to enhance the detection and deterrence of any suspicious activity.[32]

While the JEF has adopted a number of Response Options to deter threats and respond to crises, only two have been activated so far. Learning from this operational experience will, however, be important in the future in order to strengthen interoperability. In the future, JEF forces could continue to build their capabilities to strengthen its credibility. Furthermore, the JEF could also work more closely with NATO's Maritime Centre for the Security of Critical Undersea Infrastructure in Northwood, ensuring deconfliction and close collaboration. The JEF's operational responsibility is likely to be best concentrated on deterring and rapidly responding to threats below the threshold of NATO's Article 5, buying time for the 32-member Alliance to respond if a crisis escalates.

6.2. Military strategy

NATO's 2022 Strategic Concept recognises the growing scale of hybrid threats against CUI. To address CUI threats, NATO aims to improve CUI security through improved intelligence, surveillance, and reconnaissance (ISR) capabilities, cyber defence, partner collaboration, and development and deployment of novel technologies, such as UUVs and remote sensing.[33]

NATO has also established new institutions to improve CUI security. In 2023, it created the Critical Undersea Infrastructure Coordination Cell in Brussels to map vulnerabilities, streamline efforts between governments and the private sector and create a forum for military and civilian officials, as well as business representatives.[34] To drive improved public-private collaboration on CUI protection, NATO also established the Critical Undersea Infrastructure Network in 2024.[35]

In addition, NATO also established the Maritime Centre for the Security of Critical Undersea Infrastructure at MARCOM (Northwood, UK). This centre is more operationally focused. It aims to ensure that NATO can deter and defend against hybrid attacks by improving situational awareness and response capabilities.[36]

In 2025, Secretary-General Mark Rutte announced the establishment of BALTIC SENTRY, a multi-domain activity which aims to bolster patrols of CUI by military vessels and aircraft, improve integration of

[31] Willett (2023)

[32] Joint Expeditionary Force (2024b)

[33] NATO (2022)

[34] NATO (2023)

[35] NATO (2024a)

[36] NATO (2024b)

national surveillance assets, and accelerate the deployment of UUVs to further strengthen NATO's presence at sea.[37]

NATO is particularly valuable as a mechanism for coordinated responses to shared vulnerabilities and threats, by enhancing joint naval exercises, increasing undersea surveillance and maritime patrols, and strengthening intelligence-sharing among member states to ensure a unified and robust defence posture against potential adversarial actions. NATO could also embrace its role as a facilitator of cross-sector cooperation, bringing together military, civilian, government, and private stakeholders for solution-oriented workshops or wargames focusing on hybrid and grey-zone warfare.

To further strengthen CUI security, NATO Allies should also continue to invest in and enhance their contributions to Alliance operations in terms of surface, subsea, aerial and space-based intelligence, surveillance and reconnaissance (ISR) capabilities, such as uncrewed systems, as well cyber defence capabilities. The recent establishment of a NATO Innovation Fund and the Defence Innovation Accelerator for the North Atlantic (DIANA) presents new opportunities for joint development and deployment of novel technologies that could further improve the security of CUI.

6.3. Legal frameworks, including options for redress

CUI governance is complex for several reasons. Subsea infrastructures often connect different countries and may pass through the territorial waters of others, which means that different legal regimes may apply for different parts of the infrastructure. In international waters, the principle of freedom of navigation significantly limits countries' powers to inspect or board suspicious vessels. Another source of complexity is the high number of actors involved in the operation, protection and regulation of subsea infrastructure. The question of CUI security and resilience spans several policy areas from cyber security, maritime security, telecommunications, shipping, fisheries to digital infrastructures. Lastly, many suspected acts of sabotage against CUI are carried out by vessels seemingly engaging in regular commerce, allowing malign actors to push boundaries of permissible behaviour. These limitations are increasingly being recognised by Western countries. For example, Estonia has proposed changes to maritime laws to improve the possibilities of redress.[38]

[37] NATO (2025)

[38] Sytas (2024)

7. How well is policy and co-ordination working across Whitehall departments, law enforcement and private sector actors? Are any changes needed?

Because so many players are involved in the protection of undersea infrastructure, sharing information is a vital enabler of any security, resilience or deterrence efforts.

On the public sector side, responsibilities and policy levers for CUI are diffuse, presenting coordination challenges. The Department for Science, Innovation and Technology (DSIT) is the policy lead for undersea cables, while the Department for Energy Security and Net Zero (DESNZ) leads on electricity interconnectors and oil and gas pipelines (or future CUI such as carbon capture). There are also issue-specific roles for agencies such as the Maritime and Coastguard Agency (MCA), intelligence agencies and the National Cyber Security Centre (NCSC). In practice, the Royal Navy and consequently the Ministry of Defence (MOD) hold the only military assets with which to defend or deter attacks on CUI, but without having corresponding funds to do this and many other competing operational demands on small numbers of available aircraft, ships and submarines.

Information sharing can be improved by overcoming both technical and organisational or cultural barriers, including divergent incentive structures. Private sector players may be hesitant to share information with the government if it suggests they have been negligent in the protection of their subsea assets. Sharing government information with industry can also be challenging, with much of it classified and stakeholders not always incentivised to share information, particularly about potential vulnerabilities. In other words, even if the information could be shared, doing so may inadvertently expose sensitive details, such as indications about the presence of a submarine in the area that was able to gather the information. Therefore, the effective sharing of information hinges on building a climate of trust between different players, which has to grow organically. While ongoing efforts to deepen coordination between the public and private sectors at both the national and EU or NATO levels are welcome, they must go further to address the scale of the challenge.

It is important to highlight that while existing initiatives have significantly improved from a few years ago, they remain a work in progress. In response to the rapidly evolving threat landscape, a plethora of initiatives for protecting CUI have been set up at the national and international levels and in the private sector. Better delineation of tasks and sustained cooperation are necessary to ensure comprehensive protection of CUI. As a result, some elements of the protection of CUI may be covered by multiple duplicative efforts, while other issues remain unaddressed. Even as coordination improves, it may be difficult to reduce the number of initiatives, as each player is keen to signal that it is taking action.

8. In the context of limited resources, what is the appropriate balance to strike between enhancing domestic resilience on the one hand, and improving detection and interdiction on the other?

With UK Government finances under strain—and even with plans to raise defence spending to 2.5% of GDP by diverting funds from overseas aid—there remains insufficient budget to address all pressing needs such as the urgent requirements to modernise UK Armed Forces, bolster the national contribution to NATO and expand and sustain support to Ukraine.[39] As such, when various other military capabilities urgently need to be updated and strengthened, expanding specific CUI-related capabilities (e.g., specialised undersea infrastructure inspection and repair vessels) may be deprioritised.

It is also important to consider operational trade-offs. Faced with an evolving threat landscape, the UK Armed Forces are asked to undertake a growing number of tasks with finite resources. If assets are deployed for the protection of subsea assets, these assets are no longer available to take on other tasks. Given the extensive scale of critical undersea infrastructure, assets dedicated to this task may need to focus solely on it. This creates a need to balance the allocation of resources between safeguarding undersea infrastructure and addressing the many other demands on security and defence assets. Assigning crewed naval assets to undertake lengthy patrols of CUI implies opportunity costs that only serve adversaries' interests, as hostile actors can tie up high-value NATO assets on low-effort CUI missions with relatively little effort. As such, more sustainable long-term solutions are required, including using assets with less relevance to warfighting and exploiting advances in uncrewed systems, AI, sensors and other technologies. In addition, the protection of CUI is not just a "defence problem" but rather a question of national resilience. As such, it requires a cross-government solution involving at least the MOD, DSIT, DESNZ, the MCA, intelligence agencies and the NCSC, and each of these government stakeholders should allocate a portion of their budget to this effort.

The private sector must take on a greater role in safeguarding critical undersea infrastructure and adopt a duty of care. The operators of such infrastructure should serve as the first line of defence against hybrid warfare. This means making this infrastructure resilient and secure by design and considering these principles throughout the lifecycle of assets. This should include the integration of advanced monitoring techniques in CUI. If private sector companies detect any disruptions or anomalies, they should proactively

[39] Nevett et al. (2025)

share this with the relevant national and international authorities. Companies should also actively participate in coordination efforts, risk assessments and strategic planning exercises with private sector-facing authorities such as NATO's Critical Undersea Infrastructure Coordination Cell.[40]

This evidence submission primarily focuses on undersea telecommunications cables, but it is important to recognise that the critical undersea infrastructure (CUI) landscape encompasses various other types, such as undersea power cables and oil and gas pipelines. As outlined in Section 5, different types of CUI have distinct characteristics and may lead to varying impacts when disrupted. Furthermore, the cascading effects of such disruptions suggest that a simultaneous failure of multiple CUI types could result in more extensive and prolonged disruptions to essential societal services than disruptions to a single type of CUI. Therefore, protecting CUI demands a comprehensive approach that addresses all types of critical undersea infrastructure.

[40] van Soest et al. (2025)

References

Allison, George. 2023. *Britain's new undersea cable protection ship arrives*. UK Defence Journal. As of 03 March 2025: https://ukdefencejournal.org.uk/britains-new-undersea-cable-protection-ship-arrives/

Bekkers, Frank, Joris Teer, Dorith Kool, Lucia van Geuns, Patrick Bolder, Irina Patrahau, and Max Sarel. 2021. *The High Value of the North Sea*. The Hague: The Hague Centre for Strategic Studies. As of 03 March 2025: https://hcss.nl/report/high-value-of-the-north-sea/

Besch, Sophia and Erik Brown. 2024. *Securing Europe's Subsea Data Cables.* Carnegie Endowment for International Peace. As of 03 March 2025: https://carnegieendowment.org/research/2024/12/securing-europes-subsea-data-cables?lang=en

Bilinski, Hanna. 2025. *Officials emphasize importance of protecting submarine cables at RightsCon 2025.* Radio Taiwan Intl. As of 03 March 2025: https://en.rti.org.tw/news/view/id/2012518

Bueger, Christian, Tobias Liebetrau, and Jonas Franken. 2022. 'Security threats to undersea communications cables and infrastructure – consequences for the EU'. *European Parliament*. As of 03 March 2025: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Bueger, Christian and Tobias Liebetrau. 2023. 'Critical maritime infrastructure protection: What's the trouble?' *Marine Policy*, Volume 155. As of 12 June 2024: https://www.sciencedirect.com/science/article/pii/S0308597X23003056

Buljan, Adrijana. 2023. Taiwan to Get Its First Subsea Power Cable Factory in 2027. OffshoreWind.Biz. As of 03 March 2025: https://www.offshorewind.biz/2023/02/24/taiwan-to-get-its-first-subsea-power-cable-factory-in-2027/

Fisher, Lars. 2022. 'Frequent Breaks in Undersea Pipelines Mean Fixes Are Possible for Nord Stream.' *Scientific American,* 5 October. As of 12 June 2024: https://www.scientificamerican.com/article/frequent-breaks-in-undersea-pipelines-mean-fixes-are-possible-for-nord-stream/

Detecon. 2013. *Economic Impact of Submarine Cable Disruptions.* Report prepared for the Asia-Pacific Economic Cooperation. Bangkok: Detecon Asia-Pacific. As of 12 June 2024: https://www.apec.org/docs/default-source/Publications/2013/2/Economic-Impact-of-Submarine-Cable-Disruptions/2013_psu_-Submarine-Cables.pdf

Gerstein, Daniel M. and Erin N. Leidy, Emerging Technology and Risk Analysis: The Space Domain and Critical Infrastructure, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-A2875-1, 2025. As of March 4, 2025: https://www.rand.org/pubs/research_reports/RRA2875-1.html

Johnson, Keith. 2024. *The Houthis' Next Target May Be Underwater.* Foreign Policy. As of 03 March 2025: https://foreignpolicy.com/2024/02/07/houthi-red-sea-attacks-submarine-cables/

Joint Expeditionary Force. 2024a. 'History of the JEF.' As of 12 June 2024: https://jefnations.org/about-the-jef/history-of-the-jef/

——— 2024b. 'NORDIC WARDEN Enhances Protection of Critical Undersea Infrastructure.' As of 09 September 2024: https://jefnations.org/2024/06/10/nordic-warden-enhances-protection-of-critical-undersea-infrastructure/

McLachlan, Mike. 2018. 'Undersea Cables and Damage Claims.' *International Union of Marine Insurance Eye Newsletter*, March. As of 12 June 2024: https://iumi.com/news/iumi-eye-newsletter-march-2018/undersea-cable-and-damage-claims

Memija, Adnan. 2024. *Jan De Nul selected for export cable installation offshore Taiwan.* Offshore Energy. As of 03 March 2025: https://www.offshore-energy.biz/jan-de-nul-selected-for-export-cable-installation-offshore-taiwan/

Nadimi, Farzin. 2023. *Under Fire in the Bab al-Mandab: Houthi Military Capabilities and U.S. Response Options.* Washington Institute for Near East Policy. As of 03 March 2025: https://www.washingtoninstitute.org/policy-analysis/under-fire-bab-al-mandab-houthi-military-capabilities-and-us-response-options

Nadimi, Farzin and Michael Knights. 2018. *The Hodeida Campaign (Part 3): Deterring Houthi Retaliation.* Washington Institute for Near East Policy. As of 03 March 2025: https://www.washingtoninstitute.org/policy-analysis/hodeida-campaign-part-3-deterring-houthi-retaliation

Navy Lookout. 2024. 'Setbacks in the Royal Navy's effort to get newly acquired auxiliary ships into service.' As of 03 March 2025: https://www.navylookout.com/setbacks-in-the-royal-navys-effort-to-get-newly-acquired-auxiliary-ships-into-service/

Navy Lookout. 2025. 'Royal Navy submarine diplomacy: sending a warning to Russia'. As of 27 January 2025: https://www.navylookout.com/royal-navy-submarine-diplomacy-sending-a-warning-to-russia/

Nevett, Joshua, Sam Francis, and Jonathan Beale. 2025. *Starmer cuts aid to fund increase in defence spending.* BBC News. As of 03 March 2025: https://www.bbc.co.uk/news/articles/clyrkkv4gd7o

North Atlantic Treaty Organization (NATO). 2022. 'NATO 2022 Strategic Concept.' As of 12 June 2024: https://www.nato.int/cps/en/natohq/topics_210907.htm

———. 2023. 'NATO stands up undersea infrastructure coordination cell.' As of 12 June 2024: https://www.nato.int/cps/en/natohq/news_211919.htm

———. 2024a. 'NATO holds first meeting of Critical Undersea Infrastructure Network'. As of 27 January 2025: https://www.nato.int/cps/en/natohq/news_225582.htm

———. 2024b. 'NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure.' As of 12 June 2024: https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

———. 2025. 'NATO launches "Baltic Sentry" to increase critical infrastructure security'. As of 27 January 2025: https://www.nato.int/cps/en/natohq/news_232122.htm

Paik, Amy and Jennifer Counter. 2024. 'International law doesn't adequately protect undersea cables. That must change.' *Atlantic Council.* As of 03 March 2025: https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/international-law-doesnt-adequately-protect-undersea-cables-that-must-change/

Runde, Daniel F., Erin L. Murphy, and Thomas Bryja. 2024. 'Safeguarding Undersea Cables: Protecting Cyber Infrastructure amid Great Power Competition.' *Center for Strategic and International Studies.* As of 03 March 2025: https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Sechrist, Michael. 2010. 'Cyberspace in Deep Water: Protecting Undersea Communications Cables by Creating an International Public–Private Partnership.' Cambridge, MA: Harvard Kennedy School Belfer Center for Science and International Affairs. As of 12 June 2024: https://www.belfercenter.org/publication/cyberspace-deep-water-protecting-undersea-communications-cables-creating-international

van Soest, Henri and Harper Fine. 2024. 'Vital Yet Vulnerable: Undersea Infrastructure Needs Better Protection.' *RAND Blog*. As of 03 March 2025: https://www.rand.org/pubs/commentary/2024/03/vital-yet-vulnerable-undersea-infrastructure-needs.html

van Soest, Henri. 2025. 'Countering Russia's "Shadow Fleet".' *The National Interest*. As of 03 March 2025: https://nationalinterest.org/feature/countering-russias-shadow-fleet-214417

van Soest, Henri, James Black, Harper Fine, Lucia Retter. Forthcoming. *Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience.* Santa Monica, Calif.: RAND. PE-A3800-1.

Sunak, Rishi. 2017. Undersea Cables: Indispensable, Insecure. London: Policy Exchange. As of 03 March 2025: https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/

Sytas, Andrius. 2024. *Maritime law has to be changed to protect undersea infrastructure, Estonia says.* Reuters. As of 03 March 2025: https://www.reuters.com/world/europe/maritime-law-has-be-changed-protect-undersea-infrastructure-estonia-says-2024-12-27/

Taiwan Ministry of Economic Affairs. 2025. *Stable Supply of Natural Gas.* As of 03 March 2025: https://www.moeaea.gov.tw/ECW/english/content/Content.aspx?menu_id=8677

Thompson, James and Jian Ming-yan. 2025. *Undersea cable linking Taiwan-Matsu disconnects again.* Focus Taiwan. As of 03 March 2025: https://focustaiwan.tw/sci-tech/202502170012

UK Parliament, "Call for Evidence: Inquiry into Undersea Cables." As of 6 March 2025: https://committees.parliament.uk/call-for-evidence/3572

Willett, Lee. 2023. 'Demonstrating Flexibility and Scale: JEF provides non-NATO options for Generating Amphibious Effects'. *European Security & Defence.* As of 09 September 2024: https://euro-sd.com/2023/07/articles/31821/jef-provides-non-nato-options-for-generating-amphibious-effects/