November 2026



The United Kingdom's Subsea Infrastructure: A threat, vulnerability and resilience profile

Dr James A. Malcolm and Dr Ioannis Chapsos

Coventry University
SALIENT
UK Research and Innovation

Acknowledgements

This report is an output from the project, Securing UK Subsea Infrastructure: Information Sharing in times of Crisis.

The project is funded by the SALIENT Hub, a funding source from the Arts and Humanities Research Council [SALIENT DF call grant number: AH/Y505316/1]. We are extremely grateful to our funders for their support for the project.

We also wish to thank all those interviewees who gave up their time to speak to us about these important issues. Your insights have been invaluable in allowing us to develop this profile.

The project's website can be accessed at:
https://wp.coventry.domains/subseasecurity/

Citations

Malcolm, J.A., & Chapsos, I. (2026). *The United Kingdom's Subsea Infrastructure: A threat, vulnerability and resilience profile.* Coventry Open Press. https://doi.org/10.18552/CPS/2026/0003

Copyright (c) James A. Malcolm & Ioannis Chapsos, 2026.

This report is published under the Creative Commons license CC BY, except Figure 2 which is reproduced under the Creative Commons license CC BY-SA.

Authors



Dr James A. Malcolm is an Assistant Professor in the Centre for Peace and Security, Coventry University. His research focuses on security governance, critical infrastructure security and resilience, with particular expertise in maritime security and public–private cooperation.



Dr Ioannis Chapsos is an Assistant Professor in the Centre for Peace and Security, Coventry University. His research focuses on transnational organised crime in maritime contexts and critical infrastructure protection, with particular expertise in responses to both traditional and contemporary maritime security challenges, and non-state actor dynamics in maritime security.

Acronyms and Abbreviations



AC:	Alternating Current
ACMA:	Atlantic Cable Maintenance Agreement
APMA:	Atlantic Private Maintenance Agreement
BBL:	Balgzand to Bacton Line
BT:	British Telecom
CLS:	Cable Landing Station
CNI:	Critical National Infrastructure
COBR:	Cabinet Office Briefing Rooms
DC:	Direct Current
DCMS:	Department for Culture, Media and Sport
DESZN:	Department for Energy Security and Net Zero
DSIT:	Department for Science, Innovation and Technology
ENCC:	Electricity National Control Centre
EEZ:	Exclusive Economic Zone
ESCA:	European Subsea Cable Association
GCHQ:	Government Communications Headquarters
GNI:	Gas Networks Ireland
ICPC:	International Cable Protection Committee
JMSC:	Joint Maritime Security Centre
MDA:	Maritime Domain Awareness
MMO	Marine Management Organisation
MoD	Ministry of Defence
NCSC:	National Cyber Security Centre
NATO:	North Atlantic Treaty Organisation
NESO:	National Energy System Operator
NMS:	Network Management System
NPSA:	National Protective Security Authority
OFCOM:	Office of Communications
OFGEM:	Office for Gas and Electricity Markets
PIG:	Pipeline Inspection Gauge
PRSI:	Pipeline Repair and Subsea Intervention
SLTE:	Submarine Line Terminal Equipment
SNIP:	Scotland-Northern Ireland Pipeline
SIRG:	Subsea Infrastructure Response Group
UK:	United Kingdom
UNCLOS:	United Nations Convention on the Law of the Sea

Table of Contents

Executive Summary 5

1. Introduction 8
A Note on Methodology 8
A Note on Terminology 9
A Note on Report Scope 9

2. UK Subsea Infrastructure 10
2.1 Critical (Maritime) Infrastructure 10
2.2 Subsea Telecommunications Cables 12
2.3 Subsea Energy Infrastructure 13
2.4 UK Governance Structures 14

3. The Threats 16
3.1 Introducing a Threat Typology for UK Subsea Infrastructure 16
3.2 Threats from Natural Sources 17
3.2.1 Geohazards 17
3.2.2 Infrastructure Degradation 17
3.3 Threats from Human Sources 18
3.3.1 Accidental Damage 18
3.3.2 Hostile Activity 19
3.3.3 The Grey Zone 20
3.4 External Factors 21
3.5 Synthesising the UK Threat Picture 21

4. The Vulnerabilities 23
4.1 Introduction 23
4.2 Vulnerabilities Associated with Infrastructure and Networks 24
4.2.1 The At-Sea Segment 24
4.2.2 The Landing Segment 25
4.2.3 Network Design 25
4.3 Vulnerabilities Associated with Wider Governance Structures 26
4.3.1 Stakeholder Complexity 26
4.3.2 Legal and Regulatory Challenges 27

5. The Resilience of UK Subsea Infrastructure 29
5.1 Defining Resilience 29
5.2 Absorptive Capacities 31
5.2.1 Domestic Activity 31
5.2.2 International Cooperation 32
5.3 Restorative Capacities 32
5.3.1 Response 32
5.3.2 Repair 34
5.4 Adaptive Capacities 35

6. Concluding Remarks and Recommendations 37

List of References 39

Executive Summary



This report provides a profile of the UK's subsea infrastructure, highlighting the core threats and vulnerabilities associated with it and reflecting on systemic resilience. The report draws on an analysis of existing academic studies, policy papers, official reports and media outputs**,** supplemented with interviews with UK government and industry representatives carried out over a ten-month period. The report's purpose is to map out the problem space in which stakeholders must operate and cooperate to ensure the continued operation of subsea systems in the face of multiple sources of potential harm.

The report illustrates the central role subsea infrastructure systems play in the functioning of the UK economy and broader society, ensuring the flow of data and energy. It explains how these systems are examples of critical national infrastructure and outlines the range of subsea infrastructure assets connected to the UK. This includes around 64 subsea telecommunications cables, 10 subsea electricity interconnectors, and three subsea gas interconnectors. The central role the private sector has in the ownership and operation of subsea infrastructure is highlighted, illustrating the importance of effective public-private cooperation. Within the UK government, responsibility for the security and resilience of subsea infrastructure falls to a range of different departments and arms-length bodies all of whom have placed increased attention on this work.

To explore the threats facing UK subsea infrastructure, the report proposes use of a threat typology that draws upon existing examples in literature but with adaptations and additions. More specifically, threats are sub-divided by their source (natural, human, external), frequency (routine, non-routine) and by intentionality; while there is also inclusion of grey zone activity and recognition of both physical/cyber and insider/outsider threats. It is recognised that available evidence shows that natural hazards (e.g. earthquakes and current abrasion) and accidents caused by fishing and anchoring are responsible for most infrastructure damage. Nevertheless, the risk of hostile activity against subsea infrastructure, particularly involving Russia, is of increasing concern. Here it is noted that grey zone activities, actions below the threshold of war characterised by plausible deniability, require particular attention.

The report also finds evidence that perceptions of threat differ between government and industry, with some concerns around over-securitisation. This serves as a reminder that a stakeholder's specific operating environment, incentive structures, experiences and expertise shapes their threat analysis. Moreover, while knowledge of potential threats is growing in government, there is a desire for more analysis to deepen understanding of which threats should be prioritised for response and why, and to determine where the negative impact of network damage and downtime would be most acute.

When it comes to the main vulnerabilities associated with UK subsea infrastructure, the report acknowledges that some equipment failure is inevitable. The difficulties of operating in the maritime domain with its vast spaces

and variable weather also makes it difficult to effectively protect and monitor subsea infrastructure, although this can also limit hostile activity. Where vulnerability is greater is in shallower coastal waters that are often busier; alongside the areas in which subsea cables and pipelines come ashore and which are more accessible. It is recognised that the security of some Cable Landing Stations continues to cause concern, particularly as some locations are where multiple cables land. Although the report finds systemic redundancy designed into both telecommunications and energy networks, specific cables carry a large proportion of the UK's international data, while some island communities within the UK remain particularly vulnerable to single points of failure. As efforts to secure UK subsea infrastructure continue, it is increasingly important to recognise how the diversity of involved stakeholders and the transnational nature of the telecommunications and energy sectors require careful organisational work to avoid unnecessary duplication of function; improve multi-actor information sharing; and manage differing incentive structures.

The report assesses the resilience of UK subsea infrastructure by exploring three core sets of capacities – absorptive, restorative and adaptive. Absorptive capacities encapsulate the anticipation, resistance and absorption of shocks. Restorative capacities encapsulate the way a system re-establishes performance after disruption. Adaptive capacities encapsulate how a system adjusts, responds and learns from disruption. We argue that preparatory work to ensure effective incident response requires a continual focus on ensuring domestic legislation and regulations can keep pace with changing circumstances. Given the inevitable time lags in such work though it is imperative government consider how to maintain industry buy-in. While we found all stakeholders willing here; it was evident there remain some challenges, including in how well industry feel they are equipped to undertake some security and resilience tasks.

When it comes to the restoration of UK subsea infrastructure networks after damage and downtime, there are well-established response and repair structures alongside welcome organisational innovations evident. For example, new structures such as the Subsea Infrastructure Response Group (SIRG) offer genuine new capacity to aid cross-government response planning. There remains a need to look at how reporting from industry to government can be made easier, with a proposed online system we note particularly welcome.

We are also of the view that more can be done to explore whether the security clearance system over-restricts some information subsequently hindering efforts at government/industry cooperation. Repairs of subsea infrastructure operate under long term commercial agreements with repairs conducted as interruptions arise. We found general satisfaction with the structures from industry, although within government there were concerns about the limitations of the model if multiple, simultaneous interruptions took place. There was a desire for more influence over repair chronology from government with an acknowledgement this would need to be discussed carefully with industry.

Finally, our analysis of the adaptive capacities of UK subsea infrastructure systems found considerable energy from government and industry has been put in to developing new mechanisms to share information within and between each other on a regular basis. Despite this there is considerable scope and added value in looking at how the wider maritime community such as fishers and pleasure craft owners can help improve collective understanding of what is happening in the maritime domain. These stakeholders remain an under-utilised resource. Similarly, there is continued scope to improve public awareness campaigns about the role and importance of subsea infrastructure to the UK economy and society and the impact of damage and downtime. Overall, there remains a need for a more strategic and multi-sectoral focus on knowledge transfer and learning lessons in relation to the security and resilience of UK subsea infrastructure that looks at medium to long term trends.

The report concludes by making the following recommendations:

- First, **public awareness of the importance of subsea infrastructure must be improved**. This is crucial to sustain buy-in for sustained investment and activity to secure UK subsea infrastructure, particularly given the hidden nature of much of that infrastructure. Subsea infrastructure systems can also be a useful case study to demonstrate to the wider public the importance of building societal resilience given their central role in energy supplies and data flows.

- Second, there is a need for a concerted effort across UK government to develop a **deeper understanding about how specific threats and vulnerabilities may interact with individual**

cables and pipelines. The report recognises that single points of failure exist and that not all infrastructure is equal in its strategic importance. Given tight government budgets and industry's requirement to ensure commercial viability, it is important to undertake work to develop a mechanism to assess and prioritise threat/vulnerability for subsequent response planning. The typologies used in this report could help to structure this work, which will also require sustained conversations with industry and the wider maritime community to ensure support.

- This leads to the third recommendation. **Mapping of all relevant stakeholders and existing information sharing mechanisms is necessary to understand who is and is not being engaged by the UK government**. There has been a proliferation of information sharing initiatives in recent years, but we have found some within industry feel disconnected from these. There is also a need to explore how links with fishing and pleasure craft communities can be nurtured. This offers two main advantages to government. First, these maritime users could provide valuable insights into activities at sea, supporting MDA and response planning. Lessons from strategic communications and community engagement activity in other security contexts such as counterterrorism could provide a useful starting point for work here. Second, given the continued significant proportion of damage to subsea infrastructure caused by accidents; work with these communities can build awareness and reduce these incidents.

- Fourth, **continued focus on strengthening the protection of the land-based segment of subsea networks is essential.** There is a need for both physical and cyber threats to be addressed with ongoing risk assessment and protective security work for cable landing stations and pipeline terminals essential. There is also a need to understand the potential insider threats in this context given the complex supply chains around network management systems. Awareness building and engagement activity with local stakeholders including police, councils and maritime users will be important.

- Fifth, **there is a need to develop the knowledge transfer and lessons learnt capacity within UK government**. There has been a proliferation of activity relating to the security and resilience of UK subsea infrastructure in recent years. While there is some cross-government coordination via the Cabinet Office, a government function focused on the medium to long term agenda would be beneficial to further improve security and resilience. This function could undertake trend analysis, highlight activity duplication, locate best practice in and outside of the UK, engage with academia and tackle cross-sectoral challenges such as multi-actor information sharing.

1. Introduction

In 2025, the United Kingdom's (UK's) National Security Strategy made clear the government's assessment that critical national infrastructure (CNI), including cables and pipelines running under the sea, would remain a target for hostile state activity.[1] Subsea infrastructure facilitates the movement of data and energy within and between countries. As the National Security Strategy emphasised, approximately 99% of the UK's international data traffic travels by subsea fibre optic cables and three quarters of the UK's gas supply comes via subsea pipelines.[2] With rising geopolitical tensions across Europe, driven heavily by the war in Ukraine, alongside a range of disruptions to subsea infrastructure, particularly in the Baltic Sea; the British government's concerns have been shared in capitals globally.

These concerns have led to new studies into the security and resilience of subsea infrastructure across Europe and beyond from national authorities, intergovernmental organisations and academic researchers.[3] This work has been essential in shedding further light on an element of CNI that can be described as the hidden arteries of the global economy as their often remote, maritime locations render them out of sight and on occasion, out of mind. This is not to say the importance of subsea infrastructure security, particularly in times of conflict, hasn't been previously considered, it has. Prominent in the UK context was the Parliamentary National Security Strategy's (Joint Committee) report into cable security in 2025, that began to examine the threats to subsea telecommunication cables and made recommendations to government to improve their security.[4] Yet, in the context of a growth in concern about grey zone activity;[5] new reflections on subsea infrastructure security and resilience are helpful for governments and industry operators working in this space.

This report provides a profile of the UK's subsea infrastructure as a whole – cables and pipelines – highlighting the core threats and vulnerabilities associated with it and reflecting on systemic resilience. While the report is not a formal risk assessment for UK subsea infrastructure with its integrated likelihood and impact calculations, it is hoped the themes raised in this report will help underpin and structure future such assessments.

The report is an output of a Salient Research Hub project that explored multi-actor crisis information sharing in UK subsea security, funded through UK Research and Innovation.[6] The report's purpose is to map out the problem space amidst which governments, industry operators and the wider maritime community must cooperate, and underpins the project's analysis of UK information sharing practice in this context.

The report is structured as follows. In the next chapter, we provide an overview of UK subsea infrastructure assets alongside their broad governance structures. Chapter three presents a typology for conceptualising threats to subsea infrastructure networks and explores those threats most relevant to the UK. Chapter four establishes the associated vulnerabilities of UK subsea infrastructure that could be exploited, leading to operational problems. Chapter five then reflects on the resilience of UK subsea infrastructure within this established context. While there is overlap between chapters three, four and five, this structure has been chosen to help disaggregate analysis to facilitate depth. Concluding remarks and a set of recommendations help pull together the analysis.

A Note on Methodology

To build this profile, we first drew upon existing academic studies, policy papers, official reports and media outputs on subsea infrastructure security globally to locate common examples discussed in relation to threats, vulnerabilities and resilience. To improve the specificity for a UK context, we undertook interviews with UK government representatives across a range of departments/organisations that have responsibility for the security and resilience of subsea infrastructure. We also conducted interviews with representatives from the telecommunications and energy industries with a presence in the UK market. The interviews were conducted between October 2025 and July 2026 facilitating iterative data collection and analysis. This approach was further supported with presentations of emerging project findings to two security-oriented

1. UK National Security Strategy (2025), p. 15.
2. Ibid., p. 23.
3. For example, see Hendriks, M.S. & Halem, H. (2024).
4. Joint Committee on the National Security Strategy (2025a).
5. The House of Commons Defence Select Committee defines grey zone activity as, "…attacks below the threshold of war, encompassing a wide range of activities: sabotage, espionage, cyber-attacks and disinformation campaigns" (See https://committees.parliament.uk/committee/24/defence-committee/news/208271/grey-zone-threats-bring-war-to-the-doorstep-of-each-and-every-one-of-us/ [Accessed 24 August 2026]).
6. SALIENT (n.d).

working groups and one international, practitioner-led conference across the data collection period.

It should be noted that not all the issues relating to threat, vulnerabilities and resilience identified in the literature were raised by interviewees. This can be attributed to the diversity of the interview sample, including differences in sectoral affiliation (government, energy, telecommunications, and related industries), professional roles and responsibilities, levels of technical expertise, security clearance, and individual interpretations of the threat, vulnerabilities and resilience landscape. The absence of a reference to a specific threat for example within the interview data should not be interpreted as evidence that such a threat does not exist. The interviews were semi-structured with discussion kept open to facilitate conversation and allow participants to focus on their specific areas of expertise. We did not systematically prompt discussion of particular threats. Consequently, where appropriate, insights from the wider literature that have some transferability to the UK are incorporated into this profile to provide a more comprehensive assessment.

The project was reviewed and approved through Coventry University's research ethics processes, delivered through the research ethics committee of the Centre for Peace and Security, with appropriate informed consent collected and data management protocols maintained. Generative AI, specifically Microsoft Copilot, was used to help identify some initial background literature that would be relevant for this report and to brainstorm the proposed structure of the report. All sources used in this report were checked for relevance and read by the authors. All primary data collection and analysis was conducted and all report content written and edited by the authors. No collected research data was inputted into generative AI. The authors take full responsibility for the content and final layout of this report. The views and any errors remain entirely those of the authors.

A Note on Terminology

Although we use the term 'subsea infrastructure', a word evident in industry organisation names such as the European Subsea Cables Association (ESCA), the words 'undersea' and 'underwater' are regularly used to describe the same infrastructure. We make no effort to change the terminology used in literature or by interviewees where direct quotes are used, with these terms used interchangeably. On occasion we have found that terminology such as 'underwater cables' is used as a catch-all term for all infrastructure on/under the surface of the sea. Given the structural distinctions between cables and pipelines and between data and electricity cables, we prefer the word 'infrastructure' as the collective term and then highlight the practical implications of differences where relevant. We also understand 'infrastructure' as including the physical assets (cables/pipelines) and digital assets (operating systems) that make the physical assets work. When we discuss 'networks' we are discussing how these assets are connected and organised spatially and by function. Finally, when we refer to 'systems' we embrace a socio-technical conception which includes networks and the wider governance structures underpinning their operation, security and resilience. This includes all the stakeholders (owners, operators, government, users etc), their working practices, alongside relevant legislation/regulations.

A Note on Report Scope

Given our focus on physical assets and digital operating systems, the report considers both physical and cyber security. We also acknowledge that subsea infrastructure is part of wider networks, considerable proportions of which are on land. Although this land element is largely beyond the scope of this report; given the importance of these liminal spaces between land and sea for the operability of subsea infrastructure, we do consider threat, vulnerability and resilience in relation to the landing stations and coastal energy terminals through which subsea infrastructure starts and ends its maritime journey. This is not however a report that provides intricate technical operational details beyond the core information required to contextualise our security and resilience profile. It is also recognised there is some military subsea infrastructure,[7] but for reasons of national security, such information was not shared with the authors nor is it within the scope of this report. Finally, this report should be seen as capturing a snapshot in time of a constantly evolving security backdrop and growing body of research.[8] We welcome feedback on this report and encourage others to build on our work.

7. Marine Scotland Assessment (n.d).
8. We particularly hope this report can be seen as complementing the 2025 report – Subsea telecommunications cables: resilience and crisis preparedness – of the Parliamentary Committee on National Security Strategy, by including insights in the 12 months since it was published and widening focus to other examples of subsea infrastructure.

2. UK Subsea Infrastructure

2.1 Critical (Maritime) Infrastructure

The protection of critical infrastructure has long been a national priority in the UK. The UK National Protective Security Authority (NPSA) website defines critical national infrastructure (CNI) as:

> "Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:
>
> a. Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
>
> b. Significant impact on national security, national defence, or the functioning of the state".[9]

There are 13 CNI sectors, of which communications, energy and finance are three.[10] All rely on the effective functioning of subsea infrastructure, be that fibre optic data cables (communications and finance) or power cables and gas and oil pipelines (energy).

Subsea infrastructure is part of the wider body of critical infrastructure associated with the maritime domain. This infrastructure has been usefully categorised by Liebetrau and Bueger, organised by sector and location (see Figure 1).

	On the sea	In the sea	On land
Transport	Ships, shipping lanes,	Emissions	Ports
Energy	Platforms	Platforms, electricity cables, pipelines	Ports, landing stations, repair facilities
Communication	Repair ships	Data Cables	Landing stations, repair facilities
Fishery	Ships, fishing zones	Fishing gear, aquaculture	Ports, aquaculture
Eco-systems	Biodiversity	Biodiversity, carbon sink, carbon storage	Coastal areas, beaches

Figure 1: Types of Maritime Infrastructure

Source: Bueger and Liebetrau (2023), p. 3

9. National Protective Security Authority (2026).
10. Ibid.

Connected to/within the UK, there are:

- Around 64 subsea telecommunications cables.[11]
- 10 subsea electricity interconnector cables with approximately 10.3 gigawatt of operating capacity.[12]
- Three subsea gas interconnectors between the UK and other countries.[13]
- A network of subsea pipelines transporting gas within the UK and transporting oil/gas from offshore fields to land.
- A growing number of subsea cables transporting power from offshore wind farms to land with an operating capacity of over 16 gigawatts, 17% of UK energy needs.[14]

Figure 2 (subsea telecommunications cables) and Figure 3 (subsea energy infrastructure) provide a visual illustration of these networks.[15] While the number and geographic spread of these networks strengthens resilience, it should be noted that for parts of the UK – specifically its more remote island communities – there is a greater chance of falling foul of a single point of failure (see chapter 4.2.3).

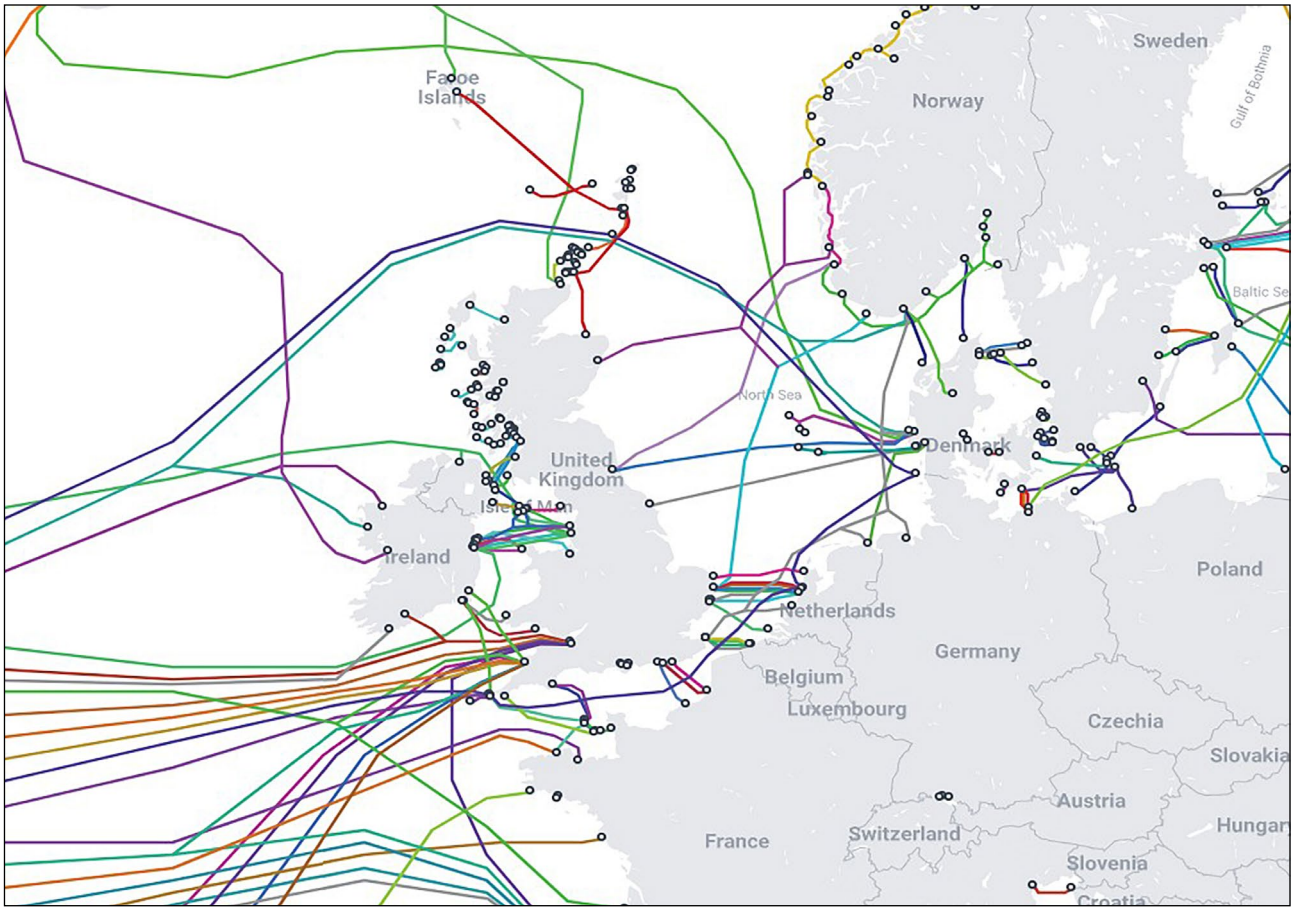


Figure 2: UK Subsea Telecommunications Cables

Source: Screenshot from TeleGeography, https://www.submarinecablemap.com/. Taken on: 24 August 2026.
This map is reproduced under Creative Commons License: Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).

11. Department for Science, Innovation and Technology (2026a). The use of the word 'around' is deliberate as the number of operational cables continually fluctuates.
12. Department for Energy Security and Net Zero (2026).
13. National Gas (2026a).
14. Renewable UK (2026).
15. As the data underpinning Figures 2 and 3 is not necessarily dynamically updated, it cannot be claimed that either figure is a completely accurate visualisation. Rather they should be understood as illustrative of network breadth.

2.2 Subsea Telecommunications Cables

Examples of operational subsea telecommunications cables with a UK connection include the ESAT-2, a 245 km cable running between Southport, UK and Sandymount, Ireland. Supplied by SubCom, it is owned and operated by Esat BT.[16] Another is CrossChannel Fibre, a fibre optic cable that came into operation in December 2021, with a 149km subsea cable running between Brighton, UK and Veules-les-Roses, France.[17] CrossChannel is a good example of the way in which subsea cables are often just one part of networks that run across land. This cable has a total length of 550km and runs between Slough, UK and Paris, France.[18] There are also subsea telecommunication cables that connect different parts of the UK. BT for example owns and operates the Highlands and Islands Submarine Cable Network, 402 km of subsea cables running across 20 seabed crossings.[19] To ensure optical signal does not lose strength along subsea telecommunications cables, in most cases repeaters restore signal approximately every 50-80 km.[20] In cables up to around 240km in length however, amplifiers at either end can boost signal.[21] Subsea telecommunications cables come onto land through Cable Landing Stations (CLSs) where Submarine Line Terminal Equipment (SLTE) "converts deep-sea optical [fibre] light signals into terrestrial electrical signals".[22] Software platforms (Network Management Systems, NMS) are used by companies to monitor and manage performance.

Subsea telecommunications cables – originally coaxial copper – have been used for over 150 years.[23] When fibre optic cables were first laid in the 1980s, it was often by state providers such as British Telecom (BT).[24] The deregulation of the telecommunications sector in the UK led to the privatisation of BT, while the birth of the internet fuelled further investment in subsea cables. Today, there are no non-military subsea telecommunications cables connecting the UK that are under public ownership and control.[25] It is an open market where companies, often with international footprints, own and operate this infrastructure. Specific ownership and operator models can vary. Cable owners often partner with landing partners, companies who would bring cables ashore and operate the wider terrestrial distribution.[26] Over the last decade the growth in content sharing platforms and artificial intelligence has resulted in big tech companies such as Google, Meta and Amazon having greater interest in subsea telecommunications cables. Their interest has shifted from buying significant proportions of capacity on cables owned and operated by consortia, towards commissioning the installation and subsequently owning and operating their own cables with near monopoly use of data capacity on them.[27]

Overall, the result is that structurally UK subsea telecommunications can be understood as being made up of a network of networks with their own inbuilt redundancies, as opposed to a single, managed UK network. Indeed, one telecommunications industry interviewee felt there was no order and structure to the current growth in capacity.[28] Contingency in the case of network downtime is ordinarily facilitated through commercial agreements between companies, while there are also emergency protocols to ensure data flows.[29] With the high demand for data continuing and subsea fibre cables often decommissioned before their planned minimum 25-year lifespan;[30] it seems likely sector growth will continue.

16. TeleGeography (2025).
17. TeleGeography (2026a).
18. Crosslake Fibre (2026).
19. Aittokallio, A. (2014).
20. KIS-ORCA (2019).
21. Ibid.
22. Qui, W. (2026).
23. European Subsea Cables Association (2026).
24. Interviewee No. 25 [April 2026].
25. UK Parliament (2023).
26. Interviewee No. 25 [April 2026].
27. Ibid.
28. Ibid.
29. Op. cit. Joint Committee on the National Security Strategy (2025a), pp. 20-21.
30. TeleGeography (2026b).

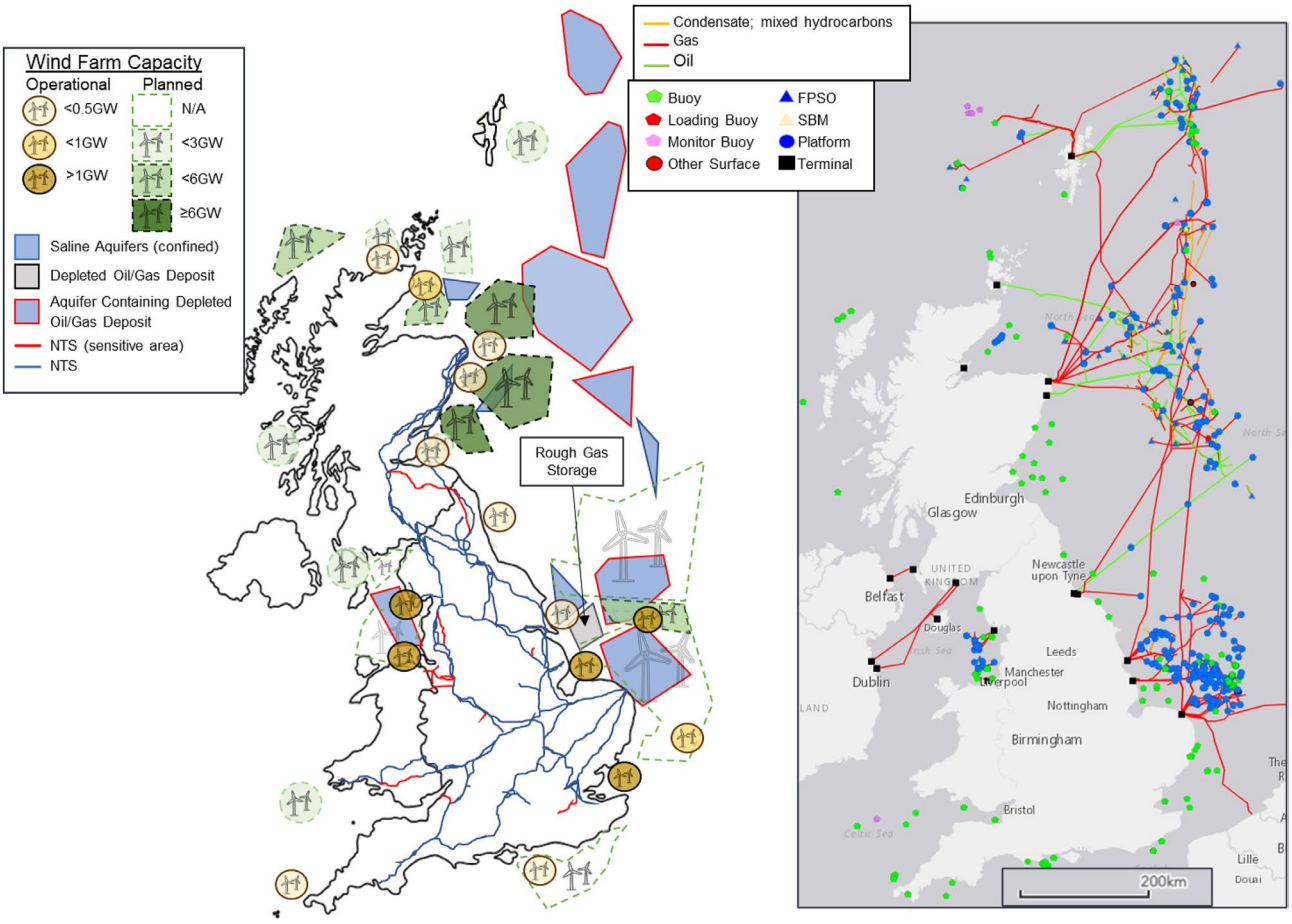


Figure 3: UK Offshore and Subsea Energy Infrastructure

Source: Wallace et al. (2021), p. 25150.

2.3 Subsea Energy Infrastructure

The number of subsea power cables connected to the UK has grown in recent years, particularly as offshore energy production has expanded. Subsea power cables sit between offshore energy assets and land, and between different countries and their respective energy grids. There are two main types of subsea power cables, alternating current (AC) and direct current (DC). AC is cheaper technology, but can travel less distance that DC, with higher voltages used to extend cable distances further.[31] Convertor facilities at each end of the subsea power cable are required to convert the voltage between DC and AC (and vice versa), with DC current common on long subsea cables and AC current used by national transmission systems.[32] Examples of electricity interconnectors between the UK and its neighbours include the Nemo Link connecting the UK and Belgium,[33] the North Sea Link between the UK and Norway,[34] and the Green Link between the UK and the Republic of Ireland.[35]

31. Op. cit. European Subsea Cables Association (2026).
32. GRIDLINK Interconnector (2021).
33. Nemolink (n.d).
34. North Sea Link (n.d).
35. Greenlink Interconnector (2025).

One gas interconnector is the Balgzand to Bacton Line (BBL) pipeline between the UK and the Netherlands.[36] Another is the INT Interconnector, a 40-inch pipeline running approximately 240 km between the UK and Belgium.[37] Both are bidirectional pipelines allowing gas to flow in both directions. The third interconnector, the Moffat Interconnector, encapsulates two unidirectional pipelines (IC1 and IC2) that send gas from Scotland to the Republic of Ireland.[38] Within the UK, one example of a subsea gas pipeline is the Scotland-Northern Ireland Pipeline (SNIP), running from Twynholm in Scotland to Ballylumford in Northern Ireland.[39] It is also unidirectional flowing from Scotland. Each of these pipelines transports processed gas and as such onshore facilities at either end often include infrastructure for the compression or decompression of the gas for wider circulation. Where gas is transported via subsea pipeline from offshore fields to the UK for processing, it will arrive at terminals before being distributed.[40] One example here is the 'FLAGS' gas pipeline that runs from the offshore Brent platforms in the north of the North Sea to St Fergus terminal in Northeast Scotland.[41] A prominent subsea oil pipeline is the Norpipe system that moves oil from Norwegian offshore oil fields in the North Sea to the UK, landing at Teesside for processing.[42] One interviewee from the energy sector noted that subsea gas was a stable industry with no growth, although they did note potential future pipeline expansion opportunities around carbon capture and/or hydrogen transportation.[43]

While the British state does not have ownership or control of any UK subsea energy infrastructure, there is more state involvement in partner countries. For example, the Viking Link subsea power cable – a 765km long, 1400 MW direct current interconnector between Lincolnshire, UK and South Jutland, Denmark – is owned and operated under a partnership model between National Grid Plc, a UK privatised entity, and Energinet, an operator owned by the Danish government.[44] Across the energy sector there is considerable variety in ownership/operations models with some infrastructure run by private consortia and some effectively under single entity control such as the Moffat Interconnector. It is owned and operated by Gas Networks Ireland (GNI), albeit through interlinked subsidiary structures dependent on the specific location of the pipelines, such as GNI UK.[45]

Overall, UK subsea energy networks are more integrated than subsea telecommunications forming a hub and spoke structure in which energy is moved through a variety of networks that feed into gas and electricity national transmission systems. The day-to-day operation of these transmission systems are managed through control centres who ensure the balance of supply and demand. Gas transmission is managed through National Gas' control room.[46] Electricity transmission is managed through the Electricity National Control Centre (ENCC), part of the National Energy System Operator (NESO).[47] National Gas is a privately owned entity, while NESO is an operationally independent state entity. NESO began work in 2024 and was established after the previously privatised entity that ran the electricity transmission system was nationalised. NESO has a range of additional functions including strategic planning around UK energy supply, security and resilience.[48]

2.4 UK Governance Structures

Both National Gas and NESO, alongside UK subsea energy network owner/operators work under frameworks managed by a national regulator, the Office for Gas and Electricity Markets (OFGEM). The regulatory frameworks for UK subsea telecommunications networks are managed by the Office of Communications (Ofcom). The day-to-day lead government department

36. BBL Company (n.d).
37. Fluxys (2026a); Fluxys (2026b).
38. Gas Networks Ireland (n.d).
39. Mutual energy (2025).
40. National Gas (2026b).
41. Shell (2026).
42. NS Energy (2022).
43. Interviewee No. 26 [June 2026].
44. Viking Link (n.d.a). NB: That is total length, not just the subsea portion.
45. Op cit. Gas Networks Ireland (n.d).
46. National Gas (2026c).
47. NESO (n.d.a).
48. NESO (n.d.b).

responsible for policy and activity relevant to UK subsea infrastructure is also dependent on the sector. Subsea energy infrastructure falls under the Department for Energy Security and Net Zero (DESNZ). During this project's data collection period, subsea data cables were the responsibility of the Department for Science, Innovation and Technology (DSIT). However, DSIT was dissolved in July 2026 by the Prime Minister. Many of the functions relevant to the resilience of networks reliant on subsea telecommunications cables are now within the Department for Culture, Media and Sport (DCMS).

Government departments with an interest in subsea infrastructure do not end with the two previously noted. The Cabinet Office, through its National Security Directorate, has responsibilities for ensuring implementation of the National Security Strategy, while it also supports the Cabinet Office Briefing Rooms (COBR) Directorate who lead on crisis response when incidents have significant national implications. The Ministry of Defence, through the Royal Navy, has at sea responsibility for protecting subsea infrastructure. While a multi-agency organisation, the Joint Maritime Security Centre (JMSC) is a central hub for data fusion and enhancing maritime domain awareness. Organisations such as the NPSA and the National Cyber Security Centre (NCSC), both part of the wider intelligence community, also provide technical expertise to enhance security and resilience.

The legal framework for governing UK subsea infrastructure security is multifaceted and constantly evolving. For subsea telecommunications, the UK remains heavily reliant on the Submarine Telegraph Act,1885, although the government has announced plans to replace this.[49] There is also legislation such as the Telecommunications (Security) Act, 2021, that establishes security and resilience standards for operators.[50] The Energy Act, 2023, plays a key role in UK energy security and was the legislation that established NESO.[51] Both subsea telecommunications and energy networks are also impacted by a range of other domestic laws. One is the National Security and Investment Act, 2021, that enables government to assess and permit/prevent business transactions in key sectors.[52] Another is the Civil Contingencies Act, 2004, that established a UK emergency planning framework.[53] There are also extensive licensing and permitting regimes in the UK that govern the installation and repairs of subsea infrastructure, with, for example, the Marine Management Organisation and Crown Estate heavily involved.[54]

It is also important to remember the international dimension to legislation and activity in this space. First there is a need for owner/operators to consider domestic legislation in the territorial waters and exclusive economic zones of all countries through which their infrastructure may pass and need repairs. For example, the subsea element of the Viking Link interconnector crosses the waters of four different countries – the UK, Netherlands, Germany and Denmark.[55] There is also international law to consider, most prominently the United Nations Convention on the Law of the Sea (UNCLOS).[56] The intricacies of UNCLOS and its role and utility in subsea infrastructure security is beyond this report, but it is worth noting that through UNCLOS, within the high seas the obligation on investigating incidents falls on the flag state of the vessel(s) in question.[57] Several of the wider implications of the legislative and jurisdictional complexity associated with the maritime domain generally, and subsea infrastructure specifically, are discussed later in this report.

---

49. Legislation.Gov.UK (2026a) and Bratby, R. (2026) ; Department for Science, Innovation and Technology (2026b).
50. Legislation.Gov.uk (2026b).
51. Department for Energy Security & Net Zero (2023).
52. Cabinet Office (2026).
53. Legislation.Gov.uk (2026c).
54. Marine Management Organisation (2026); The Crown Estate (2025).
55. Viking Link (n.d.b).
56. A helpful introduction to the debates around UNCLOS and subsea infrastructure can be found in: Ringbom, H. (2025). 'New Threats—Old Rules: Law of the Sea Issues Raised by Suspected Attacks on Submarine Infrastructure in the Baltic Sea'. *Ocean Development & International Law*, *56*(3), 390–414; and Juned M, Yani YM, Nidatya N, Darmastuti S, Astuti WRD and Sadiawati D (2026) 'Contemporary interdependence and the governance gap: the obsolescence of UNCLOS in submarine cable security'. *Front. Polit. Sci.* 8:1804572.
57. The High Seas are all parts of the sea that are not included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelagic State. [See UNCLOS Article 86].

3. The Threats

3.1 Introducing a Threat Typology for UK Subsea Infrastructure

Threats represent the sources of possible harm to the functioning of UK subsea infrastructure networks. There have been multiple efforts to categorise the threats to subsea infrastructure networks in non-UK studies. Govella for example argues that the sources of risk to undersea cables can be organised by **source** – 'natural' or 'man-made' – and by **frequency** – categorised as 'routine' or 'non-routine'.[58] Here for example, current abrasion is a natural and routine risk; an earthquake is natural and non-routine; dredging is a routine and man-made risk; whilst sabotage would be non-routine and man-made.[59] Exploring threats to subsea telecommunications cables, specifically within the European Union context, Bueger, Liebetrau and Franken also argue for categorisation by source, here described as 'origin'.[60] They have 'natural', alongside 'human' sources, and add a third category, 'external factors', that includes things outside but still related to a subsea infrastructure network's physical and digital assets, like operator bankruptcy.[61] They also sub-divide human threats by **intentionality**, distinguishing between 'accidents' such as fishing, and 'attacks' such as terrorism.[62] In the visualisation of their framework however there is no direct reference to the frequency of threats.

This report's threat categorisation framework combines the insights from the above work and then makes a couple of additions to deepen analysis further (see Figure 4). More specifically, the framework uses the three categories of threat source and the inclusion of actor intentionality from Bueger et al., alongside the frequency categorisation from Govella. Determining frequency and intentionality are challenging. The former relies on full and accurate reporting of infrastructure downtime to facilitate investigation. In the UK, we found a mixed picture around the reporting requirements and processes of potential incidents around subsea infrastructure to the UK government. Nevertheless, there is sufficient existing data and research to give a sense of threat frequency to make a base assessment. For example, within industry the International Cable Protection Committee (ICPC) has long collated fault data on subsea telecommunications cables. Between 2021 and 2025 inclusive, there recorded approximately 25 faults telecommunications cables in UK waters.[63] Ultimately, considering threat frequency can support the prioritisation of preparatory work by government and industry.

The latter – intentionality – can fall into subjective assessment if firm evidence is patchy, which in turn can prompt divergent assessments. Despite this blurriness, it remains important to consider when developing a threat profile because determinations of intentionality shape resource allocation, who responds, and under what legal framework. Moreover, the difficulties associated with formulating threat responses due to confusion around intentionality are exactly the problems those undertaking and sponsoring activity that is malicious by intent but designed to look sufficiently accidental to sow doubt prey on. This plausible deniability which creates confusion characterises grey zone activity and as such the inclusion of intentionality, however analytically challenging, is essential, especially given concerns about the growth of this activity in the maritime domain. The visualisation of the grey zone is included in our framework to emphasise its importance.

One further addition we have included in the typology is the clarification that hostile activity can be targeted at the physical and/or cyber components of subsea infrastructure networks, and that threats can have an insider and outside dimension. This focus on insider threats is common in protective security studies and has been discussed in the context of the maritime domain previously.[64] Finally, the threat typology relates to all physical and digital assets in subsea telecommunications and subsea energy networks. The likelihood and potential impact of specific threats are interwoven and do vary dependent on the specific infrastructure type and its geographic location. This is discussed more in the next chapter.

58. Govella, K. (2025).
59. Ibid.
60. Bueger, C., et al. (2022).
61. Ibid.
62. Ibid.
63. ICPC (2026) Presentation on Global Submarine Telecoms Cable Repair Data Analysis.
64. Martin, P. (2024) and Kuhn, K. et al. (2023).

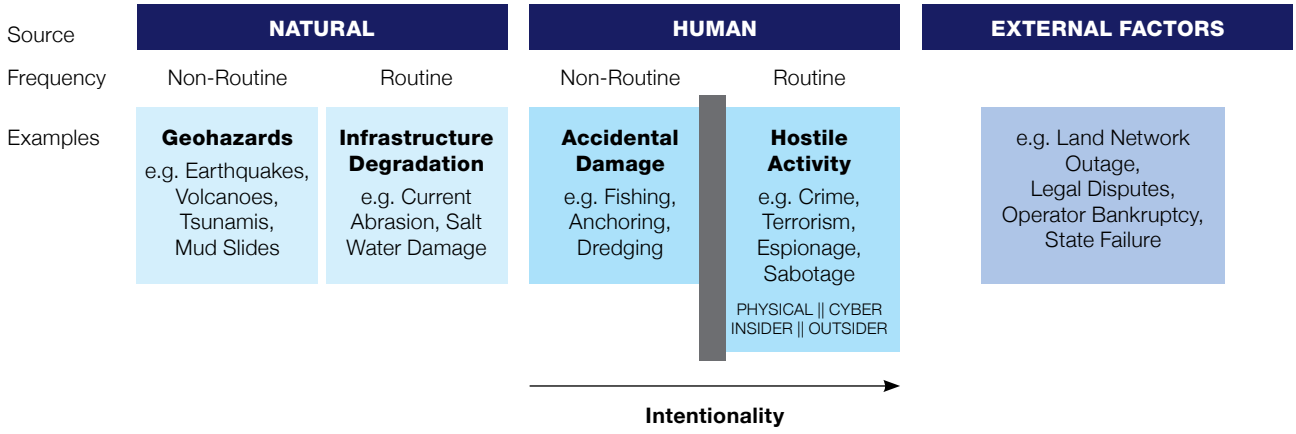


Figure 4: A Threat Typology for Subsea Infrastructure

3.2 Threats from Natural Sources

3.2.1 Geohazards

Physical subsea infrastructure assets are deployed on or beneath the seabed. This can subject both pipelines and cables to natural phenomena such as earthquakes, volcanic activity and cyclones, resulting in significant damage to infrastructure.[65] These **geohazards** are often (but not always) sudden and unpredictable and their impact can be dramatic and affect whole regions. For example, tropical cyclones damaged telecommunications cable links to Taiwan in 2009[66]; storms damaged telecommunications cables and landing stations in the Caribbean in 2017[67]; while the eruption of the Hunga Tonga-Hunga Ha'apai volcano in 2022 severed the only telecommunications cable connecting the Kingdom of Tonga to the world, isolating the country for weeks.[68] Repair data from the International Cable Protection Committee (ICPC) on subsea telecommunications cables suggests 7% of breaks globally in 2025 were caused by geological events.[69] While the UK itself sits in a relatively benign position in relation to geohazards; the fact that many of the subsea telecommunications cables that connect to it travel over significant distances and through more geologically active areas is worth noting. For example, in 2023, the West African Cable System (WACS) which moves data between the UK and South Africa via Portugal and several West African countries suffered damage due to a rock fall in the Congo Canyon, a vast submarine canyon off the coast of West Africa.[70]

3.2.2 Infrastructure Degradation

More frequent than geohazards but with a slower pace of impact as a source of harm are saltwater damage and current abrasion. The marine environment, including **saltwater,** can damage infrastructure through different forms of corrosion.[71] **Current abrasion** occurs when currents move cables around, increasing the friction against the seabed.[72] Where the seabed is rockier for example, this can result in damage to cables despite their armoured coating. ICPC data for 2025 puts the total faults caused by abrasion at 5%.[73] The risks related to the composition of the seabed varies significantly across Europe's seabed, but overall, it is considerably more rugged closer to the coastline than the ocean floor. Focusing on the UK and surrounding seas, the Baltic and North Seas are comparatively less rugged and across France's west coast, ruggedness tends to occur several kilometres offshore.[74] Within UK waters, in 2026, the rocky seabed in the Pentland Firth, contributed to the breakage of the only data cable connecting the Orkney's

65. Lazari, A. (2026).
66. Carter, L., R. Gavey, P.J. Talling, and J.T. Liu. (2014).
67. Internet Society (2018).
68. Wei-Haas M. (2022).
69. Op Cit. ICPC (2026).
70. Dux, S. (2023); Submarine Cable Networks (2024).
71. Yan, J. et al. (2026). Section 4.
72. Ibid.
73. Op Cit. ICPC (2026).
74. Franken, J. et al. (2027).

North Isles with the mainland, leaving them without internet access for almost a month.[75] As with geohazards, it is acknowledged that climate change will extenuate threats in this area.[76] The growing frequency and intensity of storms can, for example, increase seabed mobility and coastal erosion,[77] while rising sea levels are considered by the UN as a 'threat multiplier'.[78]

For operators, the degradation of their infrastructure in these environments is a recognised fact of life. Careful route planning to navigate the morphology of the seabed, alongside some protective measures such as burying infrastructure, can mitigate risks. Alongside this, careful monitoring of infrastructure to recognise problems is undertaken. One energy operator explained that they regularly use a Pipeline Inspection Gauge (PIG) to inspect the internal integrity of their gas pipeline.[79] Positive inspections have allowed the operator to essentially keep renewing the original planned 50-year service period of the pipeline.[80] Ultimately, as one energy industry interviewee explained,

> "…failures happen. There's no avoiding it. Anything that is installed will break in the end. […] Some of this is preventable with good asset management and also good installation practices. So, making sure that the cable is sufficiently buried and if necessary, protected. But you can't protect against everything. Obviously, you can't see the asset, you can't inspect it very easily. So, it's quite possible that whatever you do, the cable becomes vulnerable because the seabed shifts, etc. So, it's not a guarantee, you can just try to provide as much protection as possible…'[81]

The central implication of the inevitability of infrastructure degradation in the maritime domain is the continued need to keep increasing redundancy into the data and energy subsea systems.

3.3 Threats from Human Sources

3.3.1 Accidental Damage

Efforts to collect data on the causes of subsea cable breaks globally have consistently suggested that most breaks are caused by routine maritime activities, with fishing operations, vessel anchoring, and dredging among the most common causes of unintentional damage. The specific proportion of total breaks varies by source, with some putting it at approximately 70 per cent of annual cable breaks and others suggesting it is as high as 85 per cent.[82] This prevalence is largely attributable to operational activities conducted in close proximity to subsea infrastructure, where damage may result from limited awareness of protection zones and regulatory requirements, negligent practices, or conscious risk-taking by operators.[83] In the energy sector, between 2014 and 2017, such incidents were estimated to have resulted in approximately £250 million in lost energy production globally.[84]

The geographical distribution of **fishing-related risk** demonstrates considerable variation in both extent and intensity. Areas of elevated risk are concentrated primarily in coastal waters and in less regulated areas beyond the 200-nautical-mile Exclusive Economic Zone (EEZ) limit. Particularly high levels of fishing activity are evident around the Iberian Peninsula, within the Mediterranean Sea, and across the North Sea. By contrast, lower-risk areas are generally located further offshore in the Atlantic Ocean, as well as in parts of the Black Sea and Baltic Sea. While only some subsea cables traverse areas of particularly intense fishing activity, it is notable that the vast majority originate or terminate at landing stations situated within high-risk coastal environments.

Anchoring activity exhibits an even stronger concentration in coastal waters. Although areas of

75. BBC News (2026).
76. A study by the UK's National Oceanography Centre (NOC) argues that globally between 1965 and 2019 natural hazards collectively constituted the source of around 25% of all subsea telecommunication cable faults. See: Bricheno, L. et al. (2024).
77. Clare, M.A. et al. (2023).
78. United Nations (2021). A_76_171-EN, pp. 16/19.
79. Op Cit. Interviewee No. 26.
80. Ibid.
81. Interviewee No. 29 [May 2026].
82. Renewable UK (2018). ICPC data for 2025 put fishing and anchoring as the cause of 84% of subsea telecommunication cable faults (Op Cit. ICPC (2026)).
83. Op Cit. Bueger, C., et al. (2022).
84. Op Cit. Renewable UK (2018); Macdonald, C. et al. (2025).

elevated anchoring risk are also present away from major subsea cable routes, a consistent pattern is evident around cable landing stations, where anchoring activity is often particularly dense. High-risk concentrations are associated with major commercial ports and maritime hubs, reflecting the volume of vessel traffic and waiting areas used by commercial shipping. These patterns highlight the particular vulnerability of coastal approaches and landing infrastructure to accidental disruption arising from routine maritime operations.

In comparison, **dredging activity** displays a more limited and geographically concentrated risk profile. Its occurrence is largely confined to coastal areas, with activity concentrated around ports, navigation channels, and coastal development projects. While dredging is observed in the vicinity of some cable landing points, it is also common in coastal locations without direct connections to subsea cable networks. Overall, the spatial extent and intensity of dredging-related risk appear comparatively low when viewed across the broader European maritime region. Nevertheless, where dredging operations take place in proximity to critical subsea infrastructure, they remain a relevant source of potential disruption and therefore require appropriate consideration within risk management and protection measures.[85]

For the United Kingdom, elevated risk areas are particularly associated with heavily trafficked shipping routes and coastal waters where interaction between maritime activities and subsea infrastructure is greatest. As such, the North Sea and the English Channel emerge as areas of particular concern.[86] Collectively, the way in which routine maritime activity can inadvertently interfere with subsea infrastructure serves as a timely reminder of the importance of effective marine spatial planning, relevant public information campaigns to maritime communities highlighting areas of significant subsea infrastructure and key risks, alongside accessible reporting mechanisms for accidents.

Finally, it is important to acknowledge the potential risks posed by accidents at sea indirectly impacting subsea infrastructure. One interviewee from the UK energy sector described an incident where an oil tanker collided with another vessel in UK coastal waters directly above subsea gas pipelines. While neither vessel sank, if this had been the result, then the potential damage to the pipeline and subsequent disruption could have been significant.[87] Emergency planning must continue to recognise the ways in which the operability of subsea infrastructure may be collateral damage during **wider maritime accidents**.

3.3.2 Hostile Activity

The next set of threats to UK subsea infrastructure networks are from actors with nefarious intentions. These risks have grown as a security concern as the strategic importance of energy and telecommunications networks rise and geopolitical tensions increase. This hostile activity can be undertaken by state and non-state actors, even in collusion, seeking to disrupt critical services, undermine economic activity and/or exert political and strategic pressure.

To date, the only widely accepted act of **sabotage** of subsea infrastructure was the blowing up of the Nord Stream gas pipelines in the Baltic Sea in 2022. While the responsibility for the attacks remain unclaimed, recent developments have largely attributed then to an operation involving Ukrainian nationals.[88] The Ukrainian government has consistently denied its links to the operation.[89] Nevertheless, the Nord Stream attack was wrapped up in wider European security tensions associated with Russia's invasion of Ukraine. Russia has been accused of undertaking maritime operations in areas where European subsea infrastructure is known to be. For example, the UK government has consistently argued that Russia has undertaken **hostile reconnaissance and mapping** of its subsea infrastructure, with the Royal Navy regularly deployed to monitor and deter this activity. [90] In October 2026, an analysis by The Telegraph suggested that Russian trawler vessels were being used by the Russian government to carry out espionage on UK subsea assets.[91]

---

85. Op Cit. Franken, J. et al. (2027).
86. Ibid.
87. Interviewee No. 16 [Oct 2026].
88. Pancevski, B. (2026).
89. Cursino, M. and McGarvey, E. (2023) and Taha, R. (2026).
90. Gardner, F. (2025); Langford, C. (2026).
91. Corfield, G. et al. (2026).

Alongside physical disruption, concerns have also been raised about the **cyber threats** to subsea infrastructure networks.[92] As one interviewee working in the UK energy sector noted in interview,

> "…I guess that comes back to where I would perceive the big risk at the moment. For me, the likelihood of a third party doing anything intentionally on our on our assets, I think, is quite slim. But the likelihood of that same third party having a bash at our cyber, I think is actually quite high. You know, the nuisance value of an attack on our cyber, in terms of the volume that they have, the capacity they have, cyber is the more effective gateway for them."[93]

The cyber threat was highlighted by the UK Parliamentary report into subsea telecommunications cable security and has been the focus of recent research.[94] Franken et al. argue that cyber-attack vectors cluster around activities to disrupt the availability of services […] or to gain access to confidential data traffic.[95] In the case of the former, malicious actors could manipulate the NMS "…to stop running services, destroy relevant data, or encrypt hard drive".[96] In the case of the latter, information could be physically or remotely accessed. Here, for example, the direct tapping of subsea cables to intercept data is generally regarded as technically difficult, particularly given the challenges of operating at sea. But cable landing stations are considered more accessible and potentially attractive targets.[97] Large volumes of data are concentred in these facilities which serve as key interfaces between subsea and land-based networks. Indeed, through Project Tempora initiated in 2008, the UK's intelligence agency, The Government Communications Headquarters (GCHQ), is reported to have been able to tap up to 200 fibre-optic cables where they came ashore.[98] Analysis has also flagged the insider threat risk in a cyber context, where individuals working within organisations responsible for operating systems work from within to cause harm.[99]

3.3.3 The Grey Zone

One area of rising concern is over **grey zone activity**; actions below the threshold of war characterised by plausible deniability, whereby a protagonist can deny involvement and/or the intentionality behind an incident is unclear i.e. was it an accident or not, fuelling uncertainty. Recent incidents in the Baltic Sea, where merchant vessels have dragged their anchors over substantial distances damaging subsea infrastructure, have been the subject of much debate in this context. In October 2023, the BalticConnector gas pipeline between Estonia and Finland was damaged by an anchor drag by the NewNew Polar Bear cargo ship.[100] In December 2024, the Eagle S dragged its anchor for 93 km damaging subsea cables between Estonia and Finland.[101] Outside of Europe, similar concerns have also emerged in the Taiwan Strait, where repeated cable-cutting incidents have fuelled debate regarding the use of grey zone tactics against critical infrastructure.[102]

Grey zone activities illustrate the challenge facing states to establish intentionality or at least prove a case to the evidential standards required in a criminal court. This situation is further complicated given legal debates internationally over the extent to which states can investigate incidents outside of their territorial waters. One notable example are ongoing court judgements over the extent to which Finland has jurisdiction to bring senior officers of the Eagle S to trial. The Finnish Court of Appeal ruled in August 2026 that Finland did have jurisdiction overturning a lower court decision that they did not.[103] Investigations also rely on support from the flag state of vessels involved in incidents, which is not always forthcoming.[104] There have been particular

92. Murphy, E.L., (2025). It should be noted that subsea infrastructure could be collateral damage in broader cyber-attacks e.g. that target an energy operator's wider software systems.
93. Interviewee No. 38 [July 2026].
94. One example here is: Fenton, A. et al. (2026).
95. Franken, J. et al. in Fenton, A. et al.
96. Ibid., p. 79.
97. ENISA (2023); European Commission (2024).
98. Kessler, G. (2026), p. 32 in Op Cit. Fenton, A. et al (2026).
99. Ibid. p. 34.
100. Ahmadi, A.A. (2023).
101. Op Cit. Govella, K. (2025); Op Cit. Kessler, G. (2026), p. 31.
102. Neal, A. W. (2025); Op. Cit. Murphy, E.L (2025).
103. YLE News (2025).
104. The Flag State is the country under which a vessel is registered and whose laws are in force on board.

challenges with the so-called shadow fleet, vessels that are known to be moving Russian oil in breach of international sanctions.

For the UK, its extensive reliance on subsea infrastructure and the previously noted Russian reconnaissance of it, demands that continued focus falls on understanding the risks associated with grey zone activities. Attention must continue to be placed on reducing the opportunities for plausible deniability to flourish by enhancing maritime domain awareness and conducting deterrence and interdiction activity. UK authorities alongside infrastructure operators also need to consider the potential for low-level proxy attacks and the theft of important intellectual property.

3.4 External Factors

The third source of possible harm to the functioning of UK subsea infrastructure stems from external developments not covered elsewhere in the typology that could negatively impact operations such as the **bankruptcy of an operator** or **outages in terrestrial data or energy networks**. Given the diversity of infrastructure operators, the oversight function of regulators, and the day-to-day grid management work of actors such as NESO in the UK; the structures and processes for managing interruptions and mitigating their impact on operations are wide-ranging and well established. One energy sector interviewee for example emphasised their ongoing conversations with their lead government department, DESNZ, to discuss risk with one conversation exploring the consequences of a major offshore contractor going into administration.[105]

Navigating **legal uncertainties** is another external factor that can increase the exposure of subsea infrastructure to disruption. As many subsea cables and pipelines traverse Exclusive Economic Zones (EEZs), international waters, and in some cases disputed maritime areas; their governance and protection often involve multiple jurisdictions. This can create challenges relating to regulatory oversight, enforcement, accountability, and coordinated responses to incidents.[106] The challenge of attaining permits from non-UK countries, including near neighbours, to undertake infrastructure repairs in their waters was an issue raised by an interviewee as one source of delay.[107]

Geopolitical dynamics can also influence the development, maintenance, and security of subsea infrastructure. In regions characterised by strategic competition and territorial disputes, critical subsea assets may become vulnerable to political pressure, operational restrictions, or disruption associated with wider geopolitical rivalries. Recent developments in the Indo-Pacific illustrate this where subsea cables in SE Asia have been delayed (e.g. Southeast Asia-Japan Cable 2 (SJC2)) or even rerouted (e.g. Apricot) to avoid Chinese waters.[108] For the UK, the Russian reconnaissance of UK subsea infrastructure previously discussed is undoubtedly a wider manifestation of geopolitical tensions between the two countries. There is then a need for the UK government to keep under ongoing review how wider international developments can impact subsea infrastructure security and work with industry to understand and mitigate these risks.

3.5 Synthesising the UK Threat Picture

This chapter has illustrated the diverse range of threats to UK subsea infrastructure networks. Where it exists, data highlights that natural sources of harm and accidents remain the predominant causes of damage to physical assets. Nevertheless, given increased Russian surveillance of UK subsea infrastructure, the Nord Stream explosions, and the rise in grey zone activities internationally; it is unsurprising that the dangers of hostile activity remain high on Parliament and the government's agenda. In October 2026, the House of Commons Select Committee on Defence published a report, Defence in the High North, which highlighted how defence in this area interacts with the security of subsea infrastructure.[109] This caution is sensible given the potentially significant negative impact a co-ordinated and multi-faceted attack on UK subsea infrastructure networks could have on day-to-day life.

105. Op Cit. Interviewee No. 16.
106. Op Cit. Lazari, A. (2026).
107. Op Cit. Interviewee No. 25.
108. Weissberger, A. (2023)
109. UK Parliament (2026).

It is also important that the UK government maintains awareness of the perspectives of industry and the wider maritime community in relation to threats to subsea infrastructure. We found that different lead departments do maintain regular communications with industry, often liaising with established networks such as the European Subsea Cable Association (ESCA). We noticed differences between subsea infrastructure operators about what the principal threats to subsea infrastructure were; debates that grey zone activities undoubtedly fuel. We found an underlying worry, particularly evident across telecommunication industry participants, about the potential over-securitisation of subsea infrastructure and cable breaks. There was a sense that the focus on hostile activity from government, the media and academia was out of proportion to the number of proven incidents, while looking at more things through the prism of security could be counterproductive.

While it is important not to over-estimate the tensions here, it is nevertheless an important reminder that a stakeholder's specific operating environment, incentive structures, experiences and expertise shapes their threat analysis. There is a responsibility on government to recognise difference and explore how information sharing practices with industry can be improved to understand these differences respectfully and ensure different threat assessments do not hinder response planning. We did find some recognition within government of this challenge. One government interviewee emphasised the importance of ensuring that internal government messaging around the threats to subsea infrastructure was nuanced and that the narrative about the threat posed by hostile actors should not run ahead of the available evidence,

> "…I share the concern of industry colleagues, we've probably ended up in a place where when one of these things [a cable] goes down, the starting assumption is, oh my goodness, it's sabotage. It's, you know, it's sort of, you know, it's all kicking off. Whereas actually it's, you know, generally speaking, it's a, it's an anchor drag on or yeah, a scallop dredger. So, there is a kind of an internal communications piece".[110]

Finally, there was a consistent message from UK government interviewees that while their knowledge of the subsea infrastructure threat picture had grown markedly over the last few years, more work was required on which threats should be prioritised for response and why. This was wrapped up with efforts to assess whether some subsea infrastructure networks were more vulnerable to harm than others and to determine where the negative impact of network downtime would be most keenly felt.[111] It is to the vulnerabilities of the UK's subsea systems this report now turns.

110. Interviewee No. 31 [June 2026].
111. Interviewee No. 3 [October 2025] and Op Cit. Interviewee No. 31.

4. The Vulnerabilities

4.1 Introduction

Having discussed the sources of possible harm to UK subsea infrastructure networks, we now explore the potential vulnerabilities that could increase the susceptibility and amplify the negative impact of subsea infrastructure networks failing. Our analysis is organised into two parts. First, we examine vulnerabilities associated with the characteristics of subsea infrastructure and the wider networks they form. More specifically, we look at (a), the at-sea segment of subsea infrastructure networks i.e. everything submerged underwater; (b) the landing segment i.e. onshore receiving infrastructure; and (c) overall network design. This first part acknowledges the existence of vulnerabilities originating from the design, manufacture, installation, maintenance or repair of physical or digital assets. The second part of the chapter considers vulnerabilities that are associated with the wider governance structures underpinning UK subsea infrastructure networks and their security. Here the impact of stakeholder complexity alongside legal and regulatory challenges are discussed. Running across each part are the challenges associated with operating in the maritime domain that can compound vulnerabilities. Ultimately, failures in this space stem either from the interaction of threats and vulnerabilities or because asset originating vulnerabilities materialise. This approach is visualised in Figure 5.

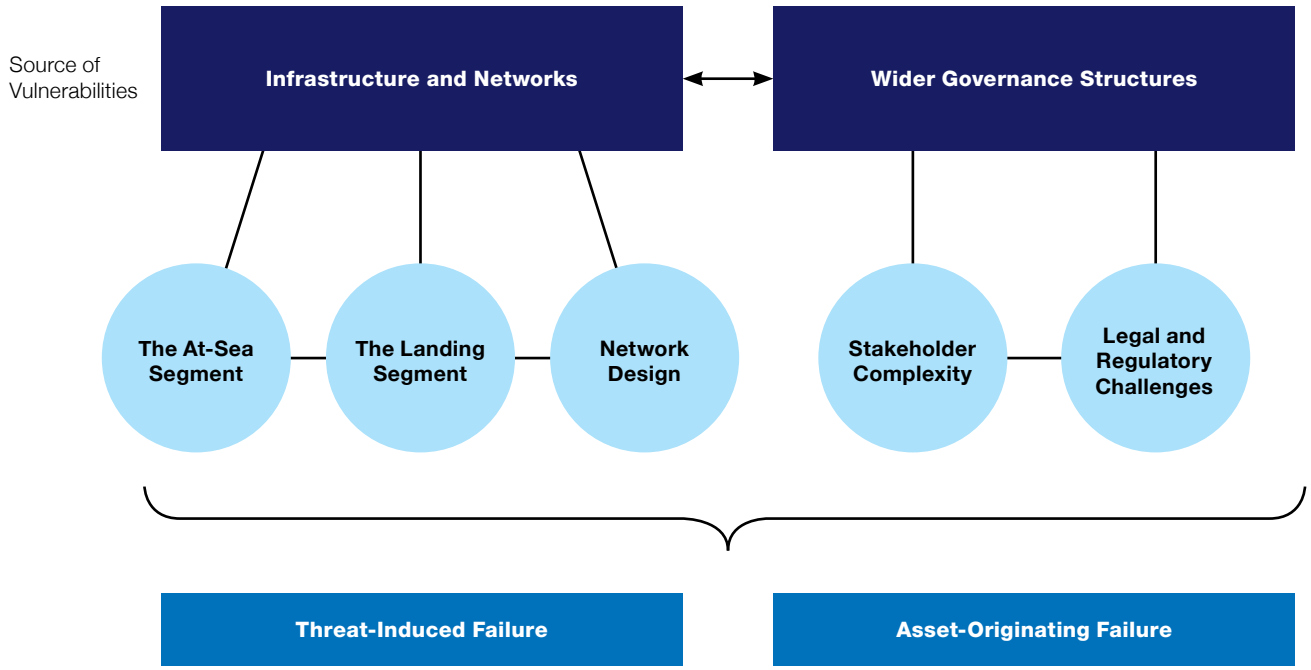


Figure 5: A Typology of UK Subsea Infrastructure System Vulnerabilities

4.2 Vulnerabilities Associated with Infrastructure and Networks

4.2.1 The At-Sea Segment

As noted in chapter 2.2, subsea telecommunications cables are usually designed to operate for up to 25 years, although they may be decommissioned earlier as technology improves. Chapter 3.2.2 noted that one of the UK's subsea gas interconnectors was also designed with a 50-year service period but that this time frame is being continually renewed after positive structural integrity reviews. While the reliability of subsea infrastructure is generally very good, it is estimated that globally about 3% of telecommunication cable faults are caused by **equipment failure.** [112] These asset originating failures are inevitable and can occur at any stage in the lifecycle of physical and digital assets. Moreover, factors such as tidal movement, seabed interaction, and weather-related currents can contribute to abrasion and wear, even if complete infrastructure failure remains relatively uncommon.[113] Despite this robustness and reliability, many assets are placed directly on the seabed or buried only shallowly beneath it, with **limited physical protection** beyond their location offshore.

The impact of threats materialising on individual assets can also differ significantly. For example, a dragged anchor on the seabed is likely to cause more damage to thinner data cables in comparison to thicker power cables, which in turn are likely to suffer more damage than if a steel gas or oil pipeline is struck. As one energy sector interviewee summarised, "…while the chance of a damage to a pipeline is maybe lesser than that to the damage of cables, the impact will be far greater".[114] This serves as an important reminder that vulnerability is not evenly distributed across subsea infrastructure networks. Indeed, one telecommunications sector interviewee noted that historically in UK and adjacent waters, a relatively small number of cable systems accounted for a disproportionately large share of recorded faults, largely because they were repeatedly exposed to damaging activities.[115]

This highlights how the **growing intensity of activity within the maritime domain** increases vulnerabilities. Interview evidence indicates that offshore areas, especially the North Sea, have become significantly busier over time; with increasing numbers of cables, pipelines, offshore renewable energy installations, survey operations, support vessels, commercial shipping movements, and fishing activity sharing the same space. This concentration of activity increases the likelihood of accidental interactions with critical infrastructure, including anchor strikes, trawling incidents, dropped objects, and vessel crossings.[116]

The characteristics of the maritime space also play a significant role in shaping both the likelihood of disruption and the effectiveness of prevention, detection, and response measures.[117] The **limited visibility and physical accessibility of subsea infrastructure** and the **challenge of building maritime situational awareness** are two further vulnerabilities to be managed. Multiple interviewees highlighted the importance of monitoring and detection as a means of establishing a baseline understanding of activity around critical subsea assets. Historically, remoteness has acted as the principal form of protection, rather than extensive hardening, continuous surveillance, or dedicated security measures. While this remoteness creates barriers for potential adversaries, it also means that infrastructure is often exposed across vast geographic areas and can make it difficult to observe activities occurring near assets in real time. Consequently, understanding what is happening around critical infrastructure often becomes the first challenge in protecting it.[118]

When incidents do occur, determining the location, nature, and cause of damage can be a lengthy and technically demanding process in the maritime domain.[119] This can also make **the attribution of incidents complex,** creating uncertainty that could be exploited by those seeking to operate in the grey zone. Moreover, operating at sea with its operational distances, changeable weather, diverse seabeds and the requirement for specialised vessels and crews, at significant cost, can make

112. Qiu, W. (2025); Op Cit. ICPC (2026).
113. Op Cit. Bueger, C., et al. (2022).
114. Interviewee No. 13 [October 2025].
115. Op Cit. Interviewee No. 25.
116. Op Cit. Interviewee No. 26.
117. Van Soest, H., et al., (2025), p. 10.
118. Op Cit. Interviewee No. 26; Interviewee No. 39 [July 2026].
119. Op Cit. Interviewee No. 29.

conducting repairs time consuming.[120] This can extenuate infrastructure downtime, even if the broader network remains operational.

4.2.2 The Landing Segment

A common theme in existing literature and our interview data is an acceptance that the areas in which subsea cables and pipelines come ashore, have increased vulnerability given the intensity of maritime activity around infrastructure in waters closer to land and **the greater physical accessibility of coastal facilities**. As it was noted in section 3.3.2, it is within these spaces that key components of the digital architecture underpinning operating systems sit and against which cyber-attacks can be targeted. These coastal facilities are generally treated as part of the UK's terrestrial CNI and are included within established risk management and emergency response processes. One prominent state actor here is the previously noted NPSA who advise industry on protective security measures.

Coastal energy terminals where gas and oil pipelines come ashore tend to be large facilities with extensive security. One energy operator explained the importance they placed on maintaining a robust security posture and outlined established protective security measures, including fencing, CCTV and 24-hour patrols, whilst noting the importance of cyber defences.[121] A similar focus on security is accepted in relation to Cable Landing Stations (CLS's), although there has been greater concern about their vulnerabilities.[122] One source of vulnerability arises from the **concentration of infrastructure and network interdependencies at specific landing locations**. Multiple subsea cables may converge on a single landing station or associated facility, meaning that disruption at one site could potentially affect several cable systems and service providers simultaneously.[123] Certain landing locations then represent critical nodes within national and international communications networks.

Another vulnerability stems from **inconsistent protective security measures** across the UK's CLS's. The level of protection has historically been inconsistent, with some facilities appearing relatively inconspicuous and receiving limited physical hardening compared with other categories of critical infrastructure. In some locations we were informed it could be possible to access coastal manholes through which data cables pass and cut them.[124] While the long-term impact of such hostile activity is likely to be limited, it is nevertheless disruptive. Franken et al. highlight one case of a minimally protected CLS in the UK where a journalist was reportedly able to access the facility through a door left open by technicians working inside.[125] This inconsistency in protective security is not unique to the UK but demonstrates that historically security through obscurity has underpinned CLS's.[126] Yet with greater awareness of the importance of CLS's, the evolving threat picture around subsea infrastructure and the wide range of stakeholders working in the system, this approach is unsustainable.

4.2.3 Network Design

As it was explained in chapter two, UK subsea energy networks are in a hub and spoke structure as electricity and gas transmission systems are monitored and balanced by national organisations, who draw on different energy sources as and when required. This can be a source of systemic redundancy given it can reduce reliance on single energy sources. However, it is worth acknowledging that there are a relatively small number of electricity and gas interconnectors. As a result, the downtime of individual assets could also have a more sustained negative impact. As one energy sector interviewee acknowledged, "[Electricity] interconnectors, by their very nature, are really kind of a single circuit again between two neighbouring countries. So again, they are very vulnerable to a specific single incident."[127]

120. Op Cit. Interviewee No. 26.
121. Op Cit. Interviewee No. 31; Interviewee No.15 [October 2025].
122. Op. cit. Joint Committee on the National Security Strategy (2025a) pp. 17-18.
123. Ibid. For example, The Joint Committee on the National Security Strategy note that nine cables land in Bude.
124. Op Cit. Interviewee No. 25.
125. Op. Cit. Franken, J. et al. in Fenton, A. et al. (2026), p. 85
126. Ibid.
127. Op Cit. Interviewee No. 26.

In relation to UK subsea telecommunications, redundancy has largely been understood to stem from the network of networks structure comprising over 60 different cables with commercial sharing agreements to manage downtime. In theory this means that ordinarily, individual or even a small group of cable breaks simultaneously are very unlikely to result in sustained, wide-ranging downtime. Nevertheless, as the UK Parliamentary Joint Committee on National Security Strategy found, two telecommunications cables account for 75% of transatlantic capacity.[128] This reminds us that as the technological capacity of cables has increased so that they can transport more data, it is not possible to argue that all data cables are necessarily of equal importance. Furthermore, the shift in who owns subsea data cables and how they operate with the growing role of big tech developing their own network, has prompted questions over the sustainability of network sharing.[129] Looking at both data and energy collectively, these debates highlight the need for ongoing dialogue between government and industry to ensure any **differences in understanding around network redundancy** do not lead to emerging vulnerabilities being missed.

Another vulnerability in network design stems from potential **single points of failure**. Some island communities within the UK rely on a single cable connection to the mainland, meaning that the loss of such infrastructure can have disproportionate consequences for local populations and economies.[130] The 2026 cable fault noted in the previous chapter due to the rocky seabed in the Pentland Firth, left around 500 customers in parts of the Orkney Islands without internet for a month.[131] One interviewee also noted the potential vulnerability of offshore wind, "There's not really an interconnected network offshore, in the same way that there is onshore. So, if you lose the cable connecting the offshore wind farm, the offshore wind farm is off." [132] Collectively this demonstrates the importance of assessing resilience not only at the national level but also at the level of individual assets, communities, and geographic regions.

The **increasing digitalisation of infrastructure operations** also creates vulnerabilities within the operating systems used to monitor, control, and maintain subsea assets. Modern networks depend upon a range of software platforms, remote management systems, and interconnected communications technologies. As a result, there are multiple points at which a cyber-attack could be targeted.[133] Cyber-related disruptions do not necessarily require hostile intent. One interviewee noted that software updates or operational mistakes have, on occasion, caused significant service outages.[134] The multiplicity of digital solutions underpinning subsea data and energy networks also highlights **the wide range of stakeholders** who feed into installing and maintaining the networks. This diversity can be a strength in helping avoid over-reliance on a single provider in instances of say, bankruptcy. But it can also increase the potential sources of insider threat for operators and government to be aware of.[135]

4.3 Vulnerabilities associated with Wider Governance Structures

4.3.1 Stakeholder Complexity

Alongside the vulnerabilities that stem from the characteristics of the subsea networks themselves, the governance of the networks can influence the situation. This report has noted **the large number of stakeholders** involved in the ownership, operation, security and resilience of UK subsea networks with a wide range of public-private partnerships. The complexity of the UK subsea telecommunications and the UK subsea energy systems is exaggerated further by the diverse range of dependent sectors on each system, the significant cross-over in stakeholders and governance between each system and their **transnational characteristics**.

128. Op. cit. Joint Committee on the National Security Strategy (2025a), p. 19.
129. Op Cit. Interviewee No. 25.
130. Op Cit. Interviewee No. 31; Interviewee No. 25.
131. Op Cit. BBC News (2026).
132. Op Cit. Interviewee No. 26.
133. US Department of State (2024); European Commission (2025).
134. Op Cit. Interviewee No. 25.
135. Op. Cit. Kessler, G. in Fenton, A. et al. (2026), p. 34.

While this complexity is not particularly unusual, it nevertheless means that responsibilities for protection, risk management, incident response, and recovery are often widely dispersed. As explained in chapter 2, within UK government there are different lead departments responsible for policy dependent on which aspect of subsea infrastructure is being considered (DESNZ/DCMS). Another department (MoD) then has responsibility for at-sea interventions, whilst another (Cabinet Office) leads on crisis response activity where there are significant national implications. This diversity can lead to a mix of expertise and experience coalescing into a holistic response. But it can also pose policymakers with the challenge of managing potential **overlaps in institutional responsibilities**, avoiding **unnecessary duplication of activity** and/or ensuring **accountability across interconnected systems.**[136] Interviewees highlighted the need to identify and manage the demarcation points where stakeholder responsibilities shift through clearly defined agreements and responsibilities, both at national and international levels. Without such arrangements, risks may emerge at the handoff points between organisations, creating ambiguity regarding accountability and operational responsibility during incidents.[137]

Ultimately stakeholders have **different mandates, capabilities and incentive structures** that underpin their priorities and practice. As one interviewee noted "… government begin to realise a number of things. They begin to realise that firstly, the risk is real and the assets aren't owned by the government, but the implications of a successful attack are owned by the government".[138] While operators recognised their responsibility for the safe operation, maintenance, and recovery of assets, we also noticed some **uncertainty regarding responsibility for protection against hostile threats**.[139] This was contrasted with the safety domain, where regulatory obligations and compliance requirements are well established.[140] These differences between stakeholders need to be understood so that policies, regulatory frameworks and communications are more responsive to specific needs.

Information sharing challenges were also evident that could make efforts to secure subsea infrastructure more challenging. A couple of energy industry interviewees expressed frustration that they had had limited communication from government or security actors about the current threat profile to their sector, about what government were doing to respond to risks or what was expected of them.[141] It was also widely acknowledged it can be difficult for government to discuss aspects of subsea security with industry because of restrictions related to security clearances. Indeed, across both telecommunications and energy it was noted that access to government assessments regarding the nature, likelihood, or evolution of threats by company boards could be better. There was acknowledgement from interviewees in government and industry that while there was some inevitability to this situation, there remained ways in which things could be improved with for example, more scrutiny within government over whether some information is over-classified.[142]

4.3.2 Legal and Regulatory Challenges

Other potential vulnerabilities can stem from gaps in the legal and/or regulatory frameworks in place around the security and resilience of subsea infrastructure. There are **questions over the deterrence impact** of the UK's legal regime around damage to subsea infrastructure. As it was noted in chapter 2 (2.4) one of the core pieces of UK legislation designed to protect subsea telecommunications cables is the Submarine Telegraph Act,1885. It does not apply beyond the territorial waters (up to 12 nautical miles);[143] while it is widely accepted to be out of date given the punishment for intentional damage is set at a maximum of five years imprisonment and culpable negligence at up to three months imprisonment or a low fine.[144] Alongside toughening these

136. Op Cit. Van Soest, H., et al., (2025), p. 10.
137. Interviewee No. 14 [October 2025].
138. Interviewee No. 37 [July 2026].
139. Ibid.; Op Cit. Interviewee No. 38.
140. Op Cit. Interviewee No. 26.
141. Op Cit. Interviewee No. 37.
142. Op Cit Interviewee No. 26; Interviewee No. 27 [April 2026]; Interviewee No. 28 [April 2026].
143. Op Cit. Joint Committee on the National Security Strategy (2025b.)
144. Legislation.Gov.UK (2026a).

penalties, new obligations will be placed on owners and operators for the physical security and resilience of their infrastructure.[145] In a sense this follows the user pays principle long established in port security.

States also must manage legal/regulatory **challenges around enforcing rules** that help protect subsea infrastructure **and investigating incidents** when damage has occurred. In the case of the former, states can, for example, monitor activity in the maritime domain via the Automatic Identification Systems (AIS) that most vessels must have on.[146] But this relies on compliance from the vessels. At times there may be legitimate reasons for a vessel going 'dark', such as a safety fear (e.g. piracy) or a technology malfunction; but these could also be used as excuses while a vessel is involved in illegal activity. This challenge of proving causality is one that grey zone activity can exploit. Coastal states seeking to investigate vessels that go dark and/or they suspect of damaging subsea infrastructure have limited powers outside of territorial waters. Instead significant responsibility falls on flag states. These flag states need to be both willing to investigate and cooperate, whilst also have domestic legislation in place to facilitate such activity. When it comes to private vessels damaging subsea infrastructure this domestic legislation is often lacking.

145. Department for Science, Innovation and Technology (2026a); Bratby, R. (2026).
146. The International Convention for the Safety of Life at Sea (SOLAS) mandates all passenger vessels and cargo vessels of a particular size must keep AIS on at all times, unless there is a valid safety reason such as a piracy threat. UK law widens this requirement to all vessels that are at least 15 metres long that are operating under the UK flag or are in UK waters. See International Maritime Organization (IMO) (1974, as amended) *International Convention for the Safety of Life at Sea (SOLAS), Chapter V, Regulation 19*. Available from: https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx (Accessed: 6 October 2026).

5. The Resilience of UK Subsea Infrastructure



5.1 Defining Resilience

With threats and vulnerabilities discussed, attention turns to the resilience of UK subsea infrastructure systems; how they might cope when something goes wrong.[147] Resilience is heavily debated with significant definitional blurriness.[148] A helpful starting point is the United Nations who define it as:

> "The ability of a system, a community or society exposed to hazards to resist absorb, accommodate to, and recover from the effect of a hazard in a timely and efficient manner including through the preservation and restoration of its essential basic structures and functions".[149]

Underpinning resilience is the acceptance that threats and vulnerabilities will materialise despite best efforts to deter, prepare and protect. As a result, the subject – in this case subsea systems – must be able to face challenges with the negative impacts mitigated as much as possible before bouncing back from adversity.

In the subsea context, Govella captures this defining "…undersea cable network resilience as the ability to mitigate risks and avoid disruptions where possible and to recover quickly from disruptions where necessary".[150] One additional component of resilience to consider is the ability of systems to learn and adapt from challenging events. Underpinned by the work of scholars such as Taleb and his work on anti-fragility;[151] including adaptation adds more dynamism to the concept, recognising that systems can have autonomy to act and evolve despite facing complex challenges.

Kavanagh, Franken and He capture all these components in their definition of resilience, outlined in their UNIDIR report on subsea cable security.[152] They present resilience as being made up of three core sets of capacities – absorptive, restorative and adaptive – which operate in a cycle to collectively enable a system to,

147. Improving resilience is just one strand of government and industry activity when it comes to subsea infrastructure. It sits alongside activity to deter hostile attacks and protect infrastructure against wider harms in the first instance.
148. Davidson, J.L. et al. (2016); Giske, M.T.E. (2021) and Atkinson, C. (2023) provide helpful summaries of these debates.
149. Op. Cit. Atkinson, C. (2023).
150. Op. Cit. Govella, K. (2025), p. 6.
151. Aven, T. (2019); Taleb, N.N. (2013).
152. Kavanagh, C., Franken, J. and He, W. (2025).

> "…anticipate, resist, absorb, respond to, and recover from negative impacts, carry out its original functions, and adapt in response to lessons learned from past experience or changed circumstances".[153]

Absorptive capacities encapsulate the anticipation, resistance and absorption of shocks. Restorative capacities encapsulate the way a system re-establishes performance after disruption. Adaptive capacities encapsulate how a system adjusts, responds and learns from disruption (see Figure 6).

Kavanagh et al. also acknowledge that there are a range of cross-cutting issues that can influence resilience. This includes the role of international law, wider international obligations, expectations of state behaviour and public/private cooperation. There is also ongoing balancing by stakeholders between say, security and resilience and national sovereignty and international cooperation, that can shape policy and practice.[154] Cross-cutting issues are discussed throughout the chapter where we have sufficient data. Also implicit throughout their approach is recognition, as noted on numerous occasions in this report so far, that operating in the maritime domain brings its own peculiarities and challenges. They provide a sample framework for governments that breaks down each set of capacities in a list of tools and practices. This focus on core capacities and the sample framework is used to help organise our UK analysis.

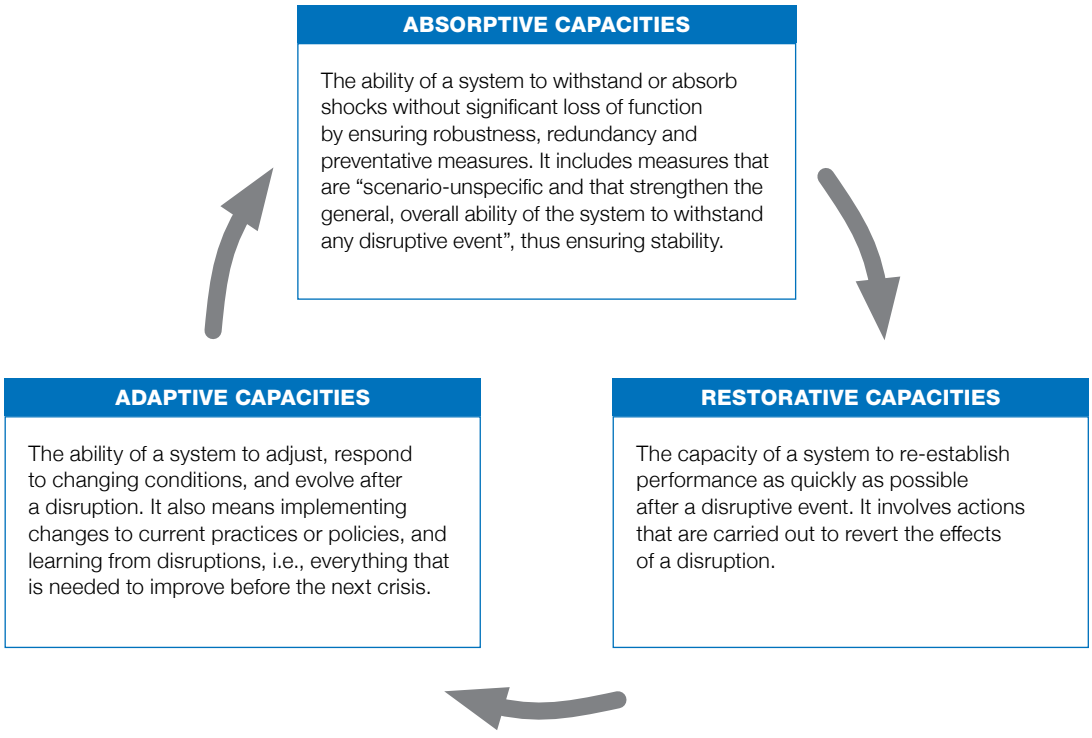


Figure 6: Core Resilience Capacities: A Cycle

Kavanagh, C., Franken, J. and He, W. (2025), p. 14.

153. Ibid. p. 7.
154. Ibid. p. 10.

5.2 Absorptive Capacities

The absorptive capacities of a system rely on the preparatory work undertaken to ensure that when an incident occurs the response is as comprehensive and timely as possible. This ensures that the shockwaves the incident initiates are more effectively managed to avoid long term and widespread system downtime.

5.2.1 Domestic Activity

Stakeholders must operate in adherence with domestic law and regulations. In broad terms, as first noted in chapter two, these may be sector specific such as The Energy Act, 2023.[155] They can be national security focused such as The National Security and Investment Act, 2021.[156] There is also emergency planning focused legislation such as The Civil Contingencies Act, 2004.[157]

We found two challenges in this area need managing. First, there is the inevitable challenge of **ensuring that legislation and regulations keep pace with changing circumstances** such as geopolitical developments or new technologies. There is an established process for developing new laws. While timeframes can be truncated in emergency situations, there remain multiple stages of Parliamentary approval and a variety of potentially competing interests to consider during the development and introduction of new legislation. The previous chapter outlined the ongoing process to review and update The Submarine Telegraph Act, 1885. A Cyber Security and Resilience Bill intended to strengthen cyber regulations is, at the time of writing, in the House of Lords for review. There is also ongoing work to better understand how existing security-facing legislation including The Telecommunications (Security) Act, 2021, may interact with the characteristics of subsea infrastructure security, and where knowledge and understanding of the maritime domain by regulators is essential.

This leads to the second challenge that **the effectiveness of law and regulations is heavily underpinned by industry buy-in about their role, alongside their capacity to meet expectations placed upon them**. This is not about industry not seeing the importance of security, they do. Nor was it about them being unwilling to invest, they are. Rather, as it has been discussed earlier in the report, some industry interviewees expressed general concerns about the over-securitisation of subsea infrastructure and shared their uncertainty and at times scepticism about the parameters of their security and resilience responsibilities given their knowledge and resources. There was also a position articulated, particularly relating to telecommunications, that the overall network design takes in to account periodic downtime caused by cable breaks, through the network of networks model, and as such breaks were not in themselves something to get overly alarmed over. As one industry interviewee summarised, "…and the whole network is designed to be able to fail over to different parts while that one part is being repaired. So, they [cable owners] don't want to be burdened with, you know, having to explain everything that's going on a day-to-day basis where, you know, the network is designed to cope with that".[158]

Sitting alongside domestic law and regulations are the wider activities undertaken to ensure government, industry and wider society are more aware of possible threats and better prepared for when incidents take place. In the context of subsea infrastructure, a core component of this preparedness work is to have **effective maritime domain awareness (MDA) so that there is a strong understanding who is operating around infrastructure, when and for what purpose**. The JMSC's role pulling together data from across UK government, industry and international partners to monitor the maritime domain in real time is essential. It was also clear from interviewees that infrastructure operators were routinely outsourcing AIS monitoring of vessels around their assets to the private sector who would flag any suspicious activity.[159] The potential role of

155. Op Cit. Department for Energy Security and Net Zero (2023).
156. Op. Cit. Cabinet Office (2026).
157. Op. Cit. Legislation.Gov.uk (2026c).
158. Interviewee No. 1 [October 2025].
159. Op Cit. Interviewee No. 38; Interviewee No. 25.

Distributed Acoustic Sensing (DAS) to advance awareness was one technological development raised during data collection, albeit with considerable debate over the efficacy of existing systems.[160] There are also industry efforts to raise awareness of the broad location of subsea infrastructure such as the KIS-ORCA publicly available map of subsea cables and offshore energy infrastructure. There are though **ongoing debates about whether it is better to pursue security through transparency or security by obscurity** when it comes to the location of subsea infrastructure. One interviewee noted they had heard that the German government had asked one of their subsea operators to remove their cables off cable charts.[161]

Alongside MDA activity, there are also regular communications between government and industry around potential threats to subsea infrastructure. We were also told about cross-government exercising in this context to work through responses to different scenarios, with plans to look at expanding these to include industry partners. Moreover, in September 2026, the UK and Republic of Ireland carried out their first joint exercise – Operation Eastern Pearl – exploring readiness in the scenario of disruption to subsea infrastructure.[162]

5.2.2 International Cooperation

UK stakeholders are also working closely with international colleagues bolstering absorptive capacities. The UK can draw on well-established wider intelligence sharing mechanisms through Five Eyes and NATO, with the latter having a designated Maritime Centre for the Security of Critical Undersea Infrastructure based at Norwood in the UK. NATO also has its Shipping Centre to liaise with merchant vessels, a CUI coordination cell in Brussels and missions such as Baltic Sentry to monitor and deter attacks in the Baltic. The UK also works with near neighbours on subsea security including through multilateral initiatives like the Joint Expeditionary Force. Bilateral partnerships are widespread and include one with Norway, formalised in December 2025 through the Lunna House Agreement, that focuses on joint naval patrols and sharing technology.[163] Industry stakeholders also play a key role in boosting preparedness internationally. Long established organisations such as the International Cable Protection Committee (ICPC) regularly meet and welcome states via observer status. There are also multilateral working groups between energy operators and governments to share insights and response planning best practice, including one around energy assets in the North Sea.

5.3 Restorative Capacities

The restorative capacities of a system rest on the extent to which those activities undertaken to manage an incident, diagnose the problem(s) and re-establish operations are effective. In the context of subsea infrastructure, we can look at response and repair.

5.3.1 Response

In the event of an incident that impacts the operation of UK subsea infrastructure, much of the preparatory work outlined in the previous section is put to the test. There remains a distinction in the characteristics of the response – who is involved and the extent of state intervention – dependent on factors such as what caused system downtime, how widespread downtime is, and the wider consequences of downtime on the economy and broader society. At the lower end of scale and impact, incident management is often left to operators to manage with regular communications with, and oversight from, government. At the other end of the spectrum, when something risks falling into potential crisis territory, this is where the UK government plays a far more active role, activating the COBR structure of whole of government response. As one government interviewee explained, COBR's involvement "…will be quite dependent on both the actual kind of the impact and what's at risk and

160. Op Cit. Interviewee No. 25; Interviewee No. 27; Interviewee No. 28. In very basic terms, fibre optic cables are used as vibration sensors. Through a DAS machine, pulses of light are sent down a fibre with vibrations in the water interrupting the amount of light reflecting creating a signature that can point to specific activity i.e. an anchor drop nearby. [Source: Science Animated (2021)].
161. Op Cit. Interviewee No. 25.
162. Lally, C. (2026).
163. GOV.UK (2025b).

whether there's going to be a branching kind of effect on the UK".[164] It is worth acknowledging that there is no fixed point at which an incident becomes a crisis, or potential crisis. Moreover, what became clear during data collection is that to date the UK has not faced a subsea infrastructure downtime event that has been deemed to have reached crisis status.

Nevertheless, **there has been significant work across government to develop response capacities**. A notable example is the creation of the 'Subsea Infrastructure Response Group' (SIRG) in the aftermath of the severing in 2022 of the SHEFA-2 telecommunications cable that connects to the Shetland Islands.[165] The SIRG is a cross-governmental response group to examine and manage subsea incidents. It was co-ordinated by DSIT when it was first established. There is also an associated industry grouping. Alongside the SIRG, the UK government developed an internal manual to ensure clarity and consistency over response processes and points of contact.[166] This sits alongside documents such as the National Emergency Plan for Subsea Fibre Optic Cables with its activation and response levels and longstanding supply planning activity by stakeholders such as NESO.[167] Bronze, Silver and Gold command structures also form a core component of incident response and understood and used by both government and industry.[168]

Despite the above, there remain questions around **the reporting of infrastructure breaks and system downtime**. In the energy sector National Gas and NESO ensure oversight of the grid. We were also told of mandatory reporting requirements in the gas industry. It was a little less clear about the extent of reporting, and whether it was mandatory or not, in relation to telecommunications outages. One industry interviewee noted information about the location of repair vessels built up their awareness of wider sector cable breaks.[169] Generally, industry communicates with the JMSC and/or their relevant government department. We were told that there is ongoing work to update and relaunch an online reporting mechanism for subsea infrastructure incidents.[170] Despite this activity, one government interviewee acknowledged incident response processes were not yet muscle memory.[171] Another industry stakeholder acknowledged there remained multiple different organisations across government seeking information and argued that having a single point of contact would be helpful:

> "So, if you asked me who was responsible in the UK for subsea security, I could probably reel off 10 people to 10 organisations who have some little finger in a pie. And then you would even then start pulling in people like OFGEM for security supply and cyber and resilience and all that sort of stuff, the NPSA, there's not one real focused, focal point, I would say. […] But if we had one body who had sole responsibility for subsea security, I think that would be, you know, that would be a really good place to start. Because like I say, if I know there's something to do with safety, I go to the health and safety executive. If there's something environmental, I go to [the] Environment Agency. For subsea security, there isn't there isn't that one responsible body".[172]

When response mechanisms are activated, a couple of further challenges were noted. First, there is an ongoing **need to recognise and manage commercial sensitivities when dealing with an incident.** We heard of some low-level tension as operators balance sharing information about the operability of their infrastructure with concerns that such information could undermine their commercial competitiveness if other operators were aware.[173] Second, **different levels of access to information across and between government and industry,** often associated with the security clearance structure, can shape response activity. More specifically, differential access influences how stakeholders establish their thresholds for reporting incidents, response prioritisation and resource allocation.

164. Op Cit. Interviewee No. 3.
165. Ibid.
166. Ibid.
167. Op Cit. Interviewee No. 25; Interviewee No. 29.
168. Op Cit. Interviewee No. 16; Interviewee No. 29.
169. Op Cit. Interviewee No. 25.
170. Op Cit. Interviewee No. 27.
171. Ibid.
172. Op Cit. Interviewee No. 26.
173. Op Cit. Interviewee No. 25.

5.3.2 Repair

In the case of cyber threats materialising, operators manage their own systems but can draw upon advice from government agencies such as the National Cyber Security Centre (NCSC). When it comes to physical damage to cables or pipelines, activity focuses on ensuring causes are investigated thoroughly and repairs are carried out speedily. ICPC data estimates the average cost of repairing a subsea fibre optic cable at between $500,000 and $1 million per incident. Repairing subsea power cables is significantly more costly at between $10 million and $100 million per incident.[174] Timelines can also vary significantly, with cables generally quicker to repair than pipelines. Van Soest et al. estimate average repair times for a subsea telecommunications cable at 7-24 days; between 40 and 60 days for an electricity interconnector; and between five and nine months to repair a subsea pipeline. [175] Here the challenges of operating at sea, particularly in challenging weather or where repairs interact with difficult seabed structures, can slow operations further.[176]

In both the telecommunications and energy sectors there are established, albeit distinct, repair frameworks. Telecommunication cable repairs generally run through maintenance and repair agreements. There are two main ones in a UK context. First, is the 'Atlantic Cable Maintenance and Repair Agreement (ACMA)', a non-profit cooperative agreement with 57 members established in 1965.[177] Through this agreement, infrastructure owners have access to three dedicated repair vessels alongside multiple stores of spare cable and equipment. The agreement covers four regions – the North Sea region, the North American region, the West African region, and the Caribbean Region.[178] The repair vessels are operated by third parties, albeit on exclusive use, and are based out of Portland, UK, Brest, France and Curacao, Netherlands Antilles.[179] Operators pay annual membership fees, a part of which are based on the number and length of their cables, alongside repair costs as and when needed.[180] Second, is the 'Atlantic Private Maintenance Agreement (APMA)', a private commercial agreement offered by cable manufacturers such as Alcatel-Lucent.[181] Network operators buy directly in to the agreement via individual maintenance contracts, with repair vessels on standby.

For energy infrastructure repairs there is also a focus on utilising a pooled support structure between owners. One example is the Pipeline Repair and Subsea Intervention (PRSI) Pool managed by the Norwegian energy operator Equinor.[182] It has 23 members who pay to be part of the pool and have access to hardware storage.[183] Equinor subcontracts services to third party providers. DeepOcean lead on pipeline repairs and subsea vessel provision, whilst Nexans and NKT hold the contract for power cable repairs.[184] Where the PRSI differs from the ACMA and APMA is that it is more geographically focused, particularly around the North Sea. The PRSI also does not have vessels on exclusive standby to its members; although one interviewee with knowledge of the pool had no concern about vessel availability, surmising the size and importance of commercial arrangements would have a clear influence in vessel deployment.[185]

Several issues need continual scrutiny to ensure effective and prompt repairs. First, industry interviewees noted **the importance of an effective approach to permitting repair vessels to operate.[186]** Some states require permits to be granted for vessels to operate, although it was noted that in the case of the UK this isn't required and operators can simply notify the Marine Management Organisation (MMO) via email that a cable will be being

174. International Cable Protection Committee (2025).
175. Op Cit., Van Soest, H. et al. (2025) p.18.
176. Op Cit. Interviewee No. 26. This interviewee also noted how a silty, muddy seabed complicated repairs of the Baltic Connector pipeline in the Baltic Sea after it was damaged. It was necessary to lay concrete mattresses first to stabilise repair equipment.
177. ACMA (n.d).
178. Ibid.
179. Ibid.
180. Ibid.
181. Burnett, D.R. (2011) pp. 67-68 and Offshore Energy (2012).
182. Op Cit. Interviewee No. 26.
183. DeepOcean (2024).
184. Op. Cit. NKT (2024) and DeepOcean (2024)
185. Op Cit. Interviewee No. 26.
186. Op Cit. Interviewee No. 1.

repaired.[187] We found satisfaction from industry about the permitting regime in the UK, although there was some anecdotal frustration about slower permitting processes in neighbouring countries.[188] Second, while both telecommunications and energy operators have access to spare hardware for repairs and some even keep some spares themselves; **continued vigilance about the strength of the supply chain around repairs is important.** Fibre optic data cables have a universal design that can improve repair times, but a small number of manufacturers of cable internationally continue to dominate the market.[189] One interviewee noted it could take around nine months for new data cables to be delivered from order.[190] It is similar for subsea electricity cables where three companies "…NKT from Denmark, Prysmian from Italy, and Nexans from France, dominate approximately 75% of the HVDC market" and each have full order books for many years into the future.[191]

Third, we noted **active debates, particularly in relation to cables, around the future availability of repair vessels and the sustainability of the workforce**. Given the significant operational area of the AMCA there was acceptance that vessels may need to travel considerable distances to carry out repairs. Moreover, vessels generally repair cables in the order in which the request for support are received.[192] There was also some acknowledgement that the relatively low number of incidents in the AMCA's operational area may result in subcontractors increasingly focusing their assets on parts of the world with more demand. One government interviewee noted that their dream "…is to be in a situation where the industry will take on government's consideration of the order of cables being repaired".[193] Related to this, acquiring a repair vessel that the UK state owned and could deploy was noted as an aspiration by the same interviewee, albeit with the acknowledgement this was likely to be cost prohibitive now.[194] This focus on a sovereign repair capacity is also wrapped up in concern over vessel availability if hostile activity proliferated. For industry, the greater concern highlighted related to a potential skills gap caused by an aging workforce in the repair sector. This was a point also noted by the Parliamentary Committee report into subsea cables that suggested a potential need to upskill Royal Navy Reservists to support repairs.[195]

5.4 Adaptive Capacities

The adaptive capacities of a system are shaped by activity that enables appropriate change and facilitates wider learning, to ensure the system is more robust in the face of future threats. To a considerable extent the focus on adapting practice to improve outcomes can and is integrated in a range of activities already discussed in this chapter. This is most obvious when stakeholders conduct exercises to test preparedness for an incident, as outlined in section 5.2.1. We found a **considerable focus from various stakeholders in building awareness of potential threats, vulnerabilities and new response initiatives**. Within government, a 'Critical Undersea Infrastructure Oversight Board' was announced to sit within the Cabinet Office to bring together actors from across government working in this space.[196] **Forums for government/industry collaboration have proliferated**. We noted some concern here. One industry stakeholder they felt a sense of compulsion to get involved in new initiatives to ensure their industry's arguments could be heard.[197] Forum shopping by stakeholders was also raised as a potential concern that could undermine long established discussion spaces that have significant institutional memory, while unnecessarily duplicating activity.

187. Op Cit. Interviewee No. 25. The Marine Management Organisation (2026) has an important role in granting licenses for subsea activity in general, while out to 12 nautical miles, the Crown Estate (2025) may also play a role as owner of the seabed.
188. Ibid.
189. For example, between 2021-2025 five manufacturers (in cable production size order) – ASN, SubCom, NEC, Elettra and HMN Technologies – collectively produced the vast majority of cable internationally. See: Submarine Telecoms Forum (2025).
190. Op Cit. Interviewee No. 1.
191. OTS Offshore (2024).
192. Op Cit. Interviewee No. 25.
193. Op Cit. Interviewee No. 3.
194. Op Cit. Interviewee No. 3.
195. Op. cit. Joint Committee on the National Security Strategy (2025a).
196. UK Parliament (2025). It is our understanding that this board largely represents a formalisation of a pre-existing function within the Cabinet Office.
197. Op Cit. Interviewee No. 25.

Where there was **less evidence of sustained engagement on subsea infrastructure security was between government, industry and wider maritime communities** such as fishers and pleasure craft users. This is a missed opportunity given the knowledge these communities have of activity in and around coastal waters in particular. There is also **scope to improve public awareness campaigns about the role and importance of subsea infrastructure to the UK economy and society and the impact of downtime**, especially in the context of efforts to enhance societal resilience.

The UK's Resilience Academy based in North Yorkshire could play a useful role here. It has given some focus to the subsea space, although there remains considerable scope for growth in activity. Local Resilience Forums can also play a key role, whilst gaining insights from countries with long established efforts to build societal resilience such as Finland would be invaluable. The UK government has recognised the **importance of informing the public of the need to prepare for emergencies** with the launch of its 'Be Ready' campaign in October 2026.[198] Overall in relation to the adaptive capacities of UK subsea infrastructure systems, while the focus on learning objectives within wider activities is welcome it is not sufficient. There remains a need for a more strategic and multi-sectoral focus on learning lessons and sharing best practice in relation to the security and resilience of UK subsea infrastructure that looks at medium to long term trends.

198. GOV.UK (2026).

6. Concluding Remarks and Recommendations

Subsea infrastructure systems are of vital importance to the UK's economy and wider society. The report has outlined that there is a plethora of threats that could interrupt the operation of UK subsea infrastructure networks. While accidents are the greatest source of damage, natural hazards, hostile activity and external events can also lead to service interruptions. All threats need to be considered by both government and industry with suitable protection and mitigation plans in place. What is also evident is that geography, including seabed morphology, has a major bearing on risk. For example, infrastructure in coastal areas closer to ports is particularly vulnerable due to the concentration of marine traffic and shallower sea depths ensuring cables and pipelines are more 'accessible'. The report has also highlighted growing concern, particularly within government, about the threat posed to subsea infrastructure by states such as Russia, particularly through the sponsoring of grey zone activity. Here the vastness of the oceans, the challenging operational conditions due to changeable weather, and the complex jurisdictional issues can make it particularly difficult to establish intentionality when subsea infrastructure is damaged.

When it comes to the vulnerability of UK subsea infrastructure and the wider networks, it is evident that cables and pipelines differ in their levels of vulnerability. Generally, cables are more vulnerable to damage than pipelines due to their smaller size, although given they are more numerous, the implications of damage to a telecommunications cable are ordinarily lower than if a gas pipeline is damaged. Cable landing stations are even more vulnerable given their wider accessibility, mixed protective security postures and their vulnerabilities to both cyber and physical threats. There are also vulnerabilities which stem from the governance structures around UK subsea infrastructure, such as when different mandates, capabilities and incentive structures impinge on stakeholder cooperation.

Despite the range of potential threats and vulnerabilities, considerable attention and resources have been placed on thinking about and improving the resilience of UK subsea infrastructure systems. This has been wrapped up in broader efforts to enhance societal resilience in the face of a more complex geopolitical environment and rising concern about challenges such as climate change. Preparations to manage damage to infrastructure and network downtime has focused on improving the legislative and regulatory framework domestically and improving cooperation with neighbouring countries. However, given the length of time it can take to implement legislative changes in particular, effort has also gone on improving maritime domain awareness and exercising to improve incident response. There remains ongoing work to ensure industry buy-in with government initiatives and we found evidence of some divergence of opinion around threat and capacities to respond.

Nevertheless, the response and repair structures for managing an incident in relation to UK subsea infrastructure are well established, with ongoing innovation evident. There remains work to do to make the reporting of damage and downtime more streamlined, although the development of the new online reporting system should help. We highlighted how some in industry remain unclear about who they should speak to for information about security and resilience. Another industry representative had more clarity here but nevertheless hoped a single point of contact responsible for UK subsea infrastructure security would be established. In the case of repairs, industry had greater concern over potential skills shortages in the repair sector, whilst within government there were concerns about the limitations of the commercial repair model if multiple, simultaneous interruptions took place.

Our analysis of the adaptive capacities of UK subsea infrastructure systems found considerable energy from government and industry had been put in to developing new mechanisms to share information within and between each other on a regular basis. There is though considerable scope and added value in looking at how the wider maritime community such as fishers and pleasure craft owners can help improve collective understanding of what is happening in the maritime domain. Similarly, there is continued scope to improve public awareness campaigns about the role and importance of subsea infrastructure to the UK economy and society and the impact of damage and downtime.

We make five recommendations:

- First, **public awareness of the importance of subsea infrastructure must be improved**. This is crucial to sustain buy-in for sustained investment and activity to secure UK subsea infrastructure, particularly

given the hidden nature of much of that infrastructure. Subsea infrastructure systems can also be a useful case study to demonstrate to the wider public the importance of building societal resilience given their central role in energy supplies and data flows.

- Second, there is a need for a concerted effort across UK government to develop a **deeper understanding about how specific threats and vulnerabilities may interact with individual cables and pipelines.** The report recognised that single points of failure exist and that not all infrastructure is equal in its strategic importance. Given tight government budgets and industry's requirement to ensure commercial viability, it is important to undertake work to develop a mechanism to assess and prioritise threat/vulnerability for subsequent response planning. The typologies used in this report could help to structure this work, which will also require sustained conversations with industry and the wider maritime community to ensure support.

- This leads to the third recommendation. **Mapping of all relevant stakeholders and existing information sharing mechanisms is necessary to understand who is and is not being engaged by the UK government**. There has been a proliferation of information sharing initiatives in recent years, but we have found some within industry feel disconnected from these. There is also a need to explore how links with fishing and pleasure craft communities can be nurtured. This offers two main advantages to government. First, these maritime users could provide valuable insights into activities at sea, supporting MDA and response planning. Lessons from strategic communications and community engagement activity in other security contexts such as counterterrorism could provide a useful starting point for work here. Second, given the continued significant proportion of damage to subsea infrastructure caused by accidents; work with these communities can build awareness and reduce these incidents.

- Fourth, **continued focus on strengthening the protection of the land-based segment of subsea networks is essential.** There is a need for both physical and cyber threats to be addressed with ongoing risk assessment and protective security work for cable landing stations and pipeline terminals essential. There is also a need to understand the potential insider threats in this context given the complex supply chains around network management systems. Awareness building and engagement activity with local stakeholders including police, councils and maritime users will be important.

- Fifth, **there is a need to develop the knowledge transfer and lessons learnt capacity within UK government**. There has been a proliferation of activity relating to the security and resilience of UK subsea infrastructure in recent years. While there is some cross-government coordination via the Cabinet Office, a government function focused on the medium to long term agenda would be beneficial to further improve security and resilience. This function could undertake trend analysis, highlight activity duplication, locate best practice in and outside of the UK, engage with academia and tackle cross-sectoral challenges such as multi-actor information sharing.

List of References

ACMA (n.d.) Atlantic Cable Maintenance Agreement [online]. Available at https://www.acma2017.com/ [Accessed 19 October 2026].

Ahmadi, A.A. (2023) Finland says gas pipeline damage probably caused by dragging anchor. *BBC News* [online]. Available from https://www.bbc.co.uk/news/world-europe-67209754 [Accessed 5 October 2026]

Aittokallio, A. (2014) 'BT completes Scottish super-fast submarine cable project', *Telecoms.com* [online] Available from https://www.telecoms.com/telecoms-infrastructure/bt-completes-scottish-super-fast-submarine-cable-project [Accessed 25 August 2026]

Atkinson, C. (2023) Research Trends in Resilience and Vulnerability Studies. *Encyclopedia 3*(4), 1208-1222, https://doi.org/10.3390/encyclopedia3040088.

Aven, T. (2019) The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Analysis*, 39: 1196-1203. https://doi.org/10.1111/risa.13247.

BBC News (2026) 'Internet access restored after Orkney broadband cable repairs' [online]. Available from https://www.bbc.co.uk/news/articles/c78lgljynyeo [Accessed 20 August 2026]

BBL Company (n.d) Transport gas in both directions between the Netherlands and Great Britain [online]. Available from https://www.bblcompany.com/ [Accessed 2 September 2026].

Bratby, R. (2026) Subsea cable security UK: DSIT plans tougher law and new operator duties. *Bratby Law* [online]. Available from https://bratby.law/subsea-cable-security-uk/ [Accessed 28 August 2026]

Bricheno, L., Yeo, I., Clare, M., Hunt, J., Griffiths, A., Carter, L., Talling, P. J., Baker, M., Wilson, S., West, M., Panuve, S., Fonua, S. (2024), The diversity, frequency and severity of natural hazard impacts on subsea telecommunications networks. *Earth-Science Reviews*, Volume 259, 104972, https://doi.org/10.1016/j.earscirev.2024.104972

Bueger, C., Liebetrau, T. (2023) Critical maritime infrastructure protection: What's the trouble?, *Marine Policy*, Volume 155, https://doi.org/10.1016/j.marpol.2023.105772

Bueger, C., Liebetrau T. and Franken, J. (2022) Security threats to undersea communications cables and infrastructure – consequences for the EU. *European Parliament, Policy Department for External Policies* [online]. Available from https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557 [Accessed 2 June 2026]

Burnett, D.R. (2011) Cable Vision. *Proceedings*, U.S. Naval Institute, Annapolis, Maryland (410) 268-6110 [online]. Available at www.usni.org [Accessed 23 October 2026].

Cabinet Office (2026) National Security and Investment Act 202. *Gov.UK* [online]. Available from https://www.gov.uk/government/collections/national-security-and-investment-act [Accessed 1 September 2026).

Carter, L., R. Gavey, P.J. Talling, and J.T. Liu. (2014) Insights into submarine geohazards from breaks in subsea telecommunication cables. *Oceanography* 27(2): 58–67, http://dx.doi.org/10.5670/oceanog.2014.40

Clare, M.A., Yeo, I.A., Bricheno, L., Aksenov, Y., Brown, J., Haigh, I.D., Wahl, T., Hunt, J., Sams, C., Chaytor, J., Bett, B.J., Carter, L. (2023) Climate change hotspots and implications for the global subsea telecommunications network. *Earth-Science Reviews* 237 (104296), https://doi.org/10.1016/j.earscirev.2022.104296

Corfield, G., Corfe, O., Sabur, R & Cotterill, T. (2026) Exclusive: Putin sends trawlers to spy on Britain. *The Telegraph* [online]. Available from https://archive.is/20261023223325/https://www.telegraph.co.uk/news/2026/10/21/exclusive-putin-sends-fishing-trawlers-to-spy-on-britain/#selection-2965.4-2965.64 [Accessed 26 October 2026].

Crosslake Fibre (2026) Crosschannel Fibre [online]. Available from https://crosslakefibre.ca/network-map/ [Accessed 25 August 2026].

Cursino, M. & McGarvey, E. (2023) Ukraine denies involvement in Nord Stream pipeline blasts. *BBC News* [online]. Available from https://www.bbc.co.uk/news/world-europe-64877979 [Accessed 21 September 2026].

Davidson, J.L. et al. (2016) Interrogating resilience: toward a typology to improve its operationalization. *Ecology and Society* 21(2):27. http://dx.doi.org/10.5751/ES-08450-210227.

DeepOcean (2024) DeepOcean awarded frame agreement for subsea infrastructure and cable repair by Equinor [online]. Available from https://www.deepoceangroup.com/articles/deepocean-awarded-frame-agreement-for-subsea-infrastructure-and-cable-repair-by-equinor [Accessed 25 October 2026].

Department for Energy Security and Net Zero (2026) Next steps for electricity interconnection in Great Britain. Policy paper [online]. Available from https://www.gov.uk/government/publications/next-steps-for-electricity-interconnection-in-great-britain/next-steps-for-electricity-interconnection-in-great-britain-accessible-webpage [Accessed 25 August 2026].

Department for Energy Security and Net Zero (2023) New laws passed to bolster energy security and deliver net zero. Press Release [online]. Available from https://www.gov.uk/government/news/new-laws-passed-to-bolster-energy-security-and-deliver-net-zero [Accessed 28 August 2026].

Department for Science, Innovation and Technology (2026a) Plan to toughen protections for subsea internet cables amid heightened Russian activity. Press release [online]. Available from https://www.gov.uk/government/news/plan-to-toughen-protections-for-subsea-internet-cables-amid-heightened-russian-activity [Accessed 25 August 2026].

Department for Science, Innovation and Technology (2026b) Plan to toughen protections for subsea internet cables amid heightened Russian activity. Press release [online]. Available from https://www.gov.uk/government/news/plan-to-toughen-protections-for-subsea-internet-cables-amid-heightened-russian-activity [Accessed on 28 August 2026].

Dux, S. (2023) Twin cable breaks impacting Southern Africa's internet. *Mobile Europe* [online]. Available from https://www.mobileeurope.co.uk/twin-cable-breaks-impacting-southern-africas-internet/ [Accessed 4 October 2026]

ENISA (2023) *Dive into the Deep Sea: A View of the Subsea Cable Ecosystem* [online]. Available from https://www.enisa.europa.eu/news/dive-into-the-deep-sea-a-view-of-the-subsea-cable-ecosystem [Accessed 30 June 2026]

European Commission (2025) EU Action Plan on Cable Security: mapping and risk assessment approach agreed by Group of Member States and Commission experts. Available online from https://digital-strategy.ec.europa.eu/en/news/eu-action-plan-cable-security-mapping-and-risk-assessment-approach-agreed-group-member-states-and [Accessed 30 June 2026]

European Commission (2024) The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World [online]. Available from https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world [Accessed 29 June 2026]

European Subsea Cables Association (2026) Submarine Telecommunication Cables [online]. Available from https://www.escaeu.org/articles/submarine-telecommunications-cables/ [Accessed 25 August 2026].

Fenton, A., Malcolm, J.A., McCabe, R. (Eds.) (2026) *CYBERCABLE: Integrating Cyber Awareness in Government and Private Sector Networks for Cooperative Critical Underwater Infrastructure Protection.* IOS Press Ebooks. Available from: https://ebooks.iospress.nl/volume/cybercable-integrating-cyber-awareness-in-government-and-private-sector-networks-for-cooperative-critical-underwater-infrastructure-protection

Fluxys (2026a) Interconnector [online] https://www.fluxys.com/en/about-us/interconnector-uk and https://www.fluxys.com/en/about-us/interconnector-uk/infrastructure (First accessed 27 August 2026).

Fluxys (2026b) Interconnector Infrastructure [online]. Available from https://www.fluxys.com/en/about-us/interconnector-uk/infrastructure [Accessed 27 August 2026].

Franken, J., Hagemeier, M., Dörnfeld, T., Löffler, J., Meissner, P., Reuter, C. (2027). SubSeaCure: Grid-Based Risk Mapping of Europe's Subsea Data Cable Network. In: Troubitsyna, E., de Andrés, D., Bitsch, F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2026. Lecture Notes in *Computer Science*, vol 16868. Springer, Cham. https://doi.org/10.1007/978-3-032-34867-8_15

Franken, J., Roth, L., Reuter, C. (2026) Information Security at Cable Landing Stations: Threats, Actors, and Protection Measures in Fenton, A. et al. (Eds.) (2026) *CYBERCABLE: Integrating Cyber Awareness in Government and Private Sector Networks for Cooperative Critical Underwater Infrastructure Protection.* IOS Press Ebooks.

Gardner, F. (2025) How serious is the Russian spy ship move? *BBC News* [online]. Available from https://www.bbc.co.uk/news/articles/c4gpgj6d4e6o [Accessed 1 July 2026]

Gas Networks Ireland (n.d) Northern Ireland [online]. Available from https://www.gasnetworks.ie/about/regulation/northern-ireland [Accessed 2 September 2026].

Giske, M.T.E. (2021) Resilience in the Age of Crises. *Norwegian Institute of International Affairs* [online]. Available from https://www.nupi.no/en/publications/cristin-pub/resilience-in-the-age-of-crises [Accessed 27 August 2026].

Govella, K. (2025). Undersea cables, geoeconomics, and security in the Indo-Pacific: Risks and resilience. *Marine Policy*, 180, 106809. https://doi.org/10.1016/j.marpol.2025.106809

GOV.UK (2025a) Cyber Security and Resilience Bill [online]. Available from https://www.gov.uk/government/collections/cyber-security-and-resilience-bill [Accessed 25 October 2026].

GOV.UK (2025b) UK and Norway to operate together to counter Russian undersea threat through major new defence agreement [online]. Available from https://www.gov.uk/government/news/uk-and-norway-to-operate-together-to-counter-russian-undersea-threat-through-major-new-defence-agreement [Accessed 9 October 2026].

GOV.UK (2026) Be Ready Campaign [online] Available from https://beready.campaign.gov.uk/ [Accessed 25 October 2026].

Greenlink Interconnector (2025) Energy security, regional investment and value for money [online]. Available from www.greenlink.ie [Accessed 27 August 2026].

GRIDLINK Interconnector (2021) Subsea and Onshore HVDC Cable Design [online]. Available from https://gridlinkinterconnector.com/project-information/design-of-the-converter-stations-and-cables/subsea-and-onshore-hvdc-cable-design/ [Accessed 2 September 2026].

Hendriks, M.S. & Halem, H. (2024) From space to seabed. *Policy Exchange.* ISBN: 978-1-910812, London

International Cable Protection Committee (2025) Damage to Submarine Cables from Dragged Anchors [online]. Available from https://www.iscpc.org/publications/icpc-viewpoints/damage-to-submarine-cables-from-dragged-anchors/ [Accessed 1 July 2026].

International Cable Protection Committee (2026) *Presentation on Global Submarine Telecoms Cable Repair Data Analysis.* Delivered to ICPC plenary in Athens, Greece.

Internet Society (2018) *Report from the Field: Post-Hurricane Connectivity in the Caribbean* [online]. Available from Report from the Field: Post-Hurricane Connectivity in the Caribbean – Internet Society [Accessed 29 June 2026]

Joint Committee on the National Security Strategy (2025a) Subsea telecommunications cables: resilience and crisis preparedness. UK Parliament [online]. Available from https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/723/report.html [Accessed 5 Oct 2026].

Joint Committee on the National Security Strategy (2025b) 'Written evidence submitted by Dr Jacques Hartmann, Professor in International Law and Human Rights, University of Dundee'. USC0040 [online]. Available from https://committees.parliament.uk/writtenevidence/139113/pdf/ [Accessed 4 October 2026]

Kavanagh, C., Franken, J. and He, W. *Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure.* Geneva: UNIDIR, 2025.

Kessler, G. (2026) Cybersecurity Challenges of Undersea Cables in Fenton, A. et al. (Eds.) (2026) *CYBERCABLE: Integrating Cyber Awareness in Government and Private Sector Networks for Cooperative Critical Underwater Infrastructure Protection.* IOS Press Ebooks.

KIS-ORCA (2019) Subsea Cables – Design [online]. Available from https://kis-orca.org/subsea-cables/design/ [Accessed 25 August 2026].

Kuhn, K., McIlhatton, D., Malcolm, J.A., Chapsos, I. (2023) Protective security at sea: a counter terrorism framework for cruise and passenger ships. *WMU J Marit Affairs* 22, 345–363. https://doi.org/10.1007/s13437-022-00296-w.

Lally, C. (2026) Irish-British governments conduct first joint exercise to plan for subsea cable attack. *The Irish Times* [online] Available from https://www.irishtimes.com/ireland/2026/09/30/irish-british-governments-conduct-first-joint-exercise-to-plan-for-subsea-cable-attack/ [Accessed 21 October 2026].

Langford, C. (2026) Russian vessels mapping UK undersea cables. *UK Defence Journal* [online] Available from https://ukdefencejournal.org.uk/russian-vessels-mapping-uk-undersea-cables/ [Accessed 1 July 2026]

Lazari, A. (2026). Critical Underwater Infrastructures: New Challenges and Threats. In: Kentera, S., Keković, Z., Čaleta, D. (eds) *Building Resilience in a Dynamic Critical Infrastructure Landscape*. NATO ARW 2025. NATO Science for Peace and Security Series C: Environmental Security. Springer, Cham. https://doi.org/10.1007/978-3-032-04383-2_3

Legislation.Gov.UK (2026a) Submarine Telegraph Act 1885 [online]. Available from https://www.legislation.gov.uk/ukpga/Vict/48-49/49#commentary-c573068 [Accessed 1 September 2026]

Legislation.Gov.Uk (2026b) Telecommunications (Security) Act 2021 [online]. Available from https://www.legislation.gov.uk/ukpga/2021/31/contents [Accessed 1 September 2026].

Legislation.Gov.UK (2026c) Civil Contingencies Act 2004 [online]. Available from https://www.legislation.gov.uk/ukpga/2004/36/contents [Accessed 1 September 2026].

Macdonald, C.; Stevens, D.; Arnhardt, R.; Carter, G.D.O.; Johnson, K.R.; Coombs, W.M.; Bird, R.E.; Augarde, C.E.; Brown, M.J.; Sharif, Y.U.. (2025) Regional analysis of layered soils in the shallow subsurface across the North Sea for offshore cable burial. In: *5th International Symposium on Frontiers in Offshore Geotechnics, Nantes, France, 9-13 June 2025*. International Society for Soil Mechanics and Geotechnical Engineering.

Marine Management Organisation (2026) Marine licensing jurisdiction. *Gov.UK* [online]. Available from https://www.gov.uk/guidance/marine-licensing-jurisdiction [Accessed 2 September 2026]

Marine Scotland Assessment (n.d.) Subsea Cables. Scottish Government [Online]. Available from https://marine.gov.scot/sma/assessment/subsea-cables [accessed 25 August 2026].

Martin, P. (2024) *Insider Risk and Personnel Security: An introduction.* Routledge: Abingdon, UK.

Murphy, E.L (2025) Redundancy, Resiliency, and Repair: Securing Subsea Cable Infrastructure. Center for Strategic & International Studies, Report, Washington DC.

Mutual energy (2025) Our gas business [online]. Available from https://www.mutual-energy.com/gas/ [Accessed 27 August 2026].

National Gas (2026a) Capacity for European connections [online]. Available from https://www.nationalgas.com/our-businesses/system-operation/capacity/capacity-european-connections [Accessed 25 August 2026].

National Gas (2026b) Gas Terminals [online]. Available from https://www.nationalgas.com/our-businesses/gas-terminals [Accessed 27 August 2026].

National Gas (2026c) National Gas Transmission [online]. Available from https://www.nationalgas.com/our-businesses/our-network-and-assets [Accessed 28 August 2026].

National Oceanography Centre (2025) 'Natural hazards responsible for 25% of subsea cable damage' [online]. Available from https://noc.ac.uk/news/natural-hazards-responsible-25-subsea-cable-damage-study-finds [Accessed 5 Oct 2026]

National Protective Security Authority (2026) Critical National Infrastructure [online]. Available from https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure [Accessed 5 Oct 2026]

Neal, A. W. (2025) After Nord Stream: four security dilemmas in critical maritime infrastructure protection. *International Affairs* 102: 1, 207–225; DOI 10.1093/ia/iiaf229

Nemolink (n.d.) European Power Distribution [online]. Available from https://www.nemolink.co.uk/ [Accessed 27 August 2026].

NESO (n.d.a) What does the Electricity National Control Centre do? [online] Available from https://www.neso.energy/what-we-do/systems-operations/what-does-electricity-national-control-centre-do [Accessed 28 August 2026].

NESO (n.d.b) About NESO [online]. Available from https://www.neso.energy/about-neso [Accessed 28 August 2026].

NKT (2024) NKT wins service agreement with Norway-based Pipeline Repair and Subsea Intervention (PRSI) Pool [online]. Available from https://www.nkt.com/news-press-releases/nkt-wins-service-agreement-with-norway-based-pipeline-repair-and-subsea-intervention-prsi-pool [Accessed 25 October 2026].

North Sea Link (n.d) The world's longest subsea interconnector linking the UK and Norway [online]. Available from https://www.northsealink.com/ [Accessed 27 August 2026].

NS Energy (2022) Norpipe Oil and Gas Pipeline [online]. Available from https://www.nsenergybusiness.com/projects/norpipe-oil-and-gas-pipeline/?cf-view [Accessed 28 August 2026].

Offshore Energy (2012) Alcatel-Lucent and Main One Extend Maintenance Contract for Portugal – Nigeria Subsea Cable [online]. Available from https://www.offshore-energy.biz/2012/12/06/alcatel-lucent-and-main-one-extend-maintenance-contract-for-portugal-nigeria-subsea-cable [Accessed 23 October 2026].

OTS Offshore (2024) Shortage of submarine power cables poses threat to offshore wind market [online] Available from https://ots-tl.com/shortage-of-submarine-power-cables-poses-threat-to-offshore-wind-market/ [Accessed 27 August 2026].

Pancevski, B. (2026) *The Nord Stream Conspiracy.* Hutchinson Heinemann: London, UK.

PWC (n.d) Understanding The Cyber Security & Resilience Bill [online]. Available from https://www.pwc.co.uk/services/technology/cyber-security-services/insights/understanding-cyber-security-and-resilience-bill.html [Accessed 25 October 2026].

Qui, W. (2026) 'FCC Overhauls Subsea Cable Licensing: SLTE Licensing and Fast-Track Process for US Tech Giants', *Submarine Cable Networks* [online]. Available from https://www.submarinenetworks.com/en/nv/insights/fcc-subsea-cable-licensing-slte-fast-tract-process [Accessed 25 August 2026].

Qiu, W. (2025) Statistics on Subsea Cable Fault and Repair. *Submarine Cable Networks* [online]. Available from https://www.submarinenetworks.com/en/nv/insights/statistics-on-subsea-cable-fault-and-repair [Accessed 5 October 2026]

Renewable UK (2026) Offshore wind [online]. Available from https://www.renewableuk.com/our-work/offshore-wind/ [Accessed 25 August 2026].

Renewable UK (2018) Offshore Wind Cable Manufacturing and Installation Forecast 2018–2028

Science Animated (2021) What is Distributed Acoustic Sensing and how does it monitor a Cable [online]. Available from: https://www.youtube.com/watch?v=9YVzMXQTFcs&t=9s [Accessed 4 October 2026].

Shell (2026) SEGAL System [online]. Available from https://www.shell.co.uk/business/oil-and-gas/segal-system.html [Accessed 27 August 2026].

Submarine Cable Networks (2024) WACS [online]. Available from https://www.submarinenetworks.com/en/systems/euro-africa/wacs [Accessed 4 October 2026]

Submarine Telecoms Forum (2025) Submarine Telecoms Industry Report 2025–2026 [online]. Available from https://subtelforum.com/submarine-telecoms-industry-report-2025-2026-out-now/ [Accessed 15 October 2026].

Taha, R. (2026) Ukraine denies involvement in Nord Stream blasts. *Deutsche Welle* [online] Available from: https://www.dw.com/en/ukraine-denies-nord-stream-sabotage/a-77894652 [Accessed 21 September 2026]

Taleb, N.N. (2013) Antifragile: Things that Gain from Disorder. Penguin: London, UK.

TeleGeography (2026a) Submarine Cable Map [online]. Available from https://www.submarinecablemap.com/submarine-cable/crosschannel-fibre [Accessed 25 August 2026].

TeleGeography (2026b) Submarine Cable Frequently Asked Questions [online]. Available from https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions [Accessed 25 August 2026].

TeleGeography (2025) Submarine Cable Map [online]. Available from https://www.submarinecablemap.com/submarine-cable/esat-2 [Accessed 25 August 2026].

The Crown Estate (2025) Marine – Cables and Pipelines [online]. Available from https://www.thecrownestate.co.uk/our-business/marine/cables-and-pipelines [Accessed 2 September 2026].

UK National Security Strategy (2025) Security for the British people in a dangerous world. *HM Government CP 1338* [online]. Available from https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html [Accessed 5 May 2026]

UK Parliament (2023) Telecommunications Cables: Seas and Oceans [online]. Available from https://questions-statements.parliament.uk/written-questions/detail/2023-05-19/HL7988/ [Accessed 25 August 2026].

UK Parliament (2025) Government strengthens undersea cables coordination following Committee report [online]. Available from https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/211009/government-strengthens-undersea-cables-coordination-following-committee-report/ [Accessed 7 October 2026].

UK Parliament (2026a) Defence in the High North [online]. Available from https://committees.parliament.uk/publications/55447/standard/pdf [Accessed 23 October 2026].

UK Parliament (2026b) Cyber Security and Resilience (Network and Information Systems) Bill [online]. Available from https://bills.parliament.uk/bills/4035 [Accessed 25 October 2026].

United Nations (2021) United Nations Informal Consultative Process on Oceans and the Law of the Sea (ICP-21) [online]. A_76_171-EN available from https://digitallibrary.un.org/record/3937016?v=pdf [Accessed 5 October 2026]

US Department of State (2024) Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World [Online]. Available from https://2021-2025.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/ [Accessed 30 June 2026]

Van Soest, H., Black, J., Fine, H., Retter L., (2025) *Evolving threats to critical undersea infrastructure: Implications for European security and resilience.* RAND Europe

Viking Link (n.d.a) About Viking link [online]. Available from https://www.viking-link.com/ [Accessed 27 August 2026].

Viking Link (n.d.b) Offshore work [online]. Available from https://www.viking-link.com/cables/offshore-work [Accessed 26 August 2026].

Wallace R.L., Cai, Z., Zhang, H., Zhang, K., Guo, C., (2021) Utility-scale subsurface hydrogen storage: UK perspectives and technology. *International Journal of Hydrogen Energy*, 46(49), 25137-25159. https://doi.org/10.1016/j.ijhydene.2021.05.034.

Wei-Haas M. (2022) 'The volcanic explosion in Tonga destroyed an island—and created many mysteries' *National Geographic* [online]. Available from The volcanic explosion in Tonga destroyed an island—and created many mysteries | National Geographic [Accessed 29 June 2026]

Weissberger, A. (2023) 'China seeks to control Asian subsea cable systems; SJC2 delayed, Apricot and Echo avoid South China Sea'. *IEEE Communication Society Technology Blog* [online]. Available from https://techblog.comsoc.org/2023/03/14/china-seeks-to-control-asian-subsea-cable-systems-apricot-and-echo-avoid-south-china-sea/ [Accessed 4 September 2026]

Yan, J., Zhang, Y., Chen, Z., Li, P., Li, Y., Cao, Z., Wu, J., Yang, K., & Zhang, D. (2026). Pipeline Systems in Floating Offshore Production Systems: Hydrodynamics, Corrosion, Design and Maintenance. *Journal of Marine Science and Engineering*, *14*(2), 176. https://doi.org/10.3390/jmse14020176

YLE News (2025) Court u-turn: Finland does have jurisdiction in Eagle S cable damage case [online]. Available from https://yle.fi/a/74-20243196 [Accessed 5 October 2026].

Interviews

Interviewee No. 1 [October 2025]

Interviewee No. 3 [October 2025]

Interviewee No. 13 [October 2025]

Interviewee No. 14 [October 2025]

Interviewee No. 15 [October 2025]

Interviewee No. 16 [Oct 2026]

Interviewee No. 25 [April 2026]

Interviewee No. 26 [June 2026]

Interviewee No. 27 [April 2026]

Interviewee No. 28 [April 2026]

Interviewee No. 29 [May 2026]

Interviewee No. 31 [June 2026]

Interviewee No. 37 [July 2026]

Interviewee No. 38 [July 2026]

Interviewee No 39 [July 2026]


Coventry
University

SALIENT

UKRI
UK Research
and Innovation