



House of Lords  
House of Commons

Joint Committee on the National Security Strategy

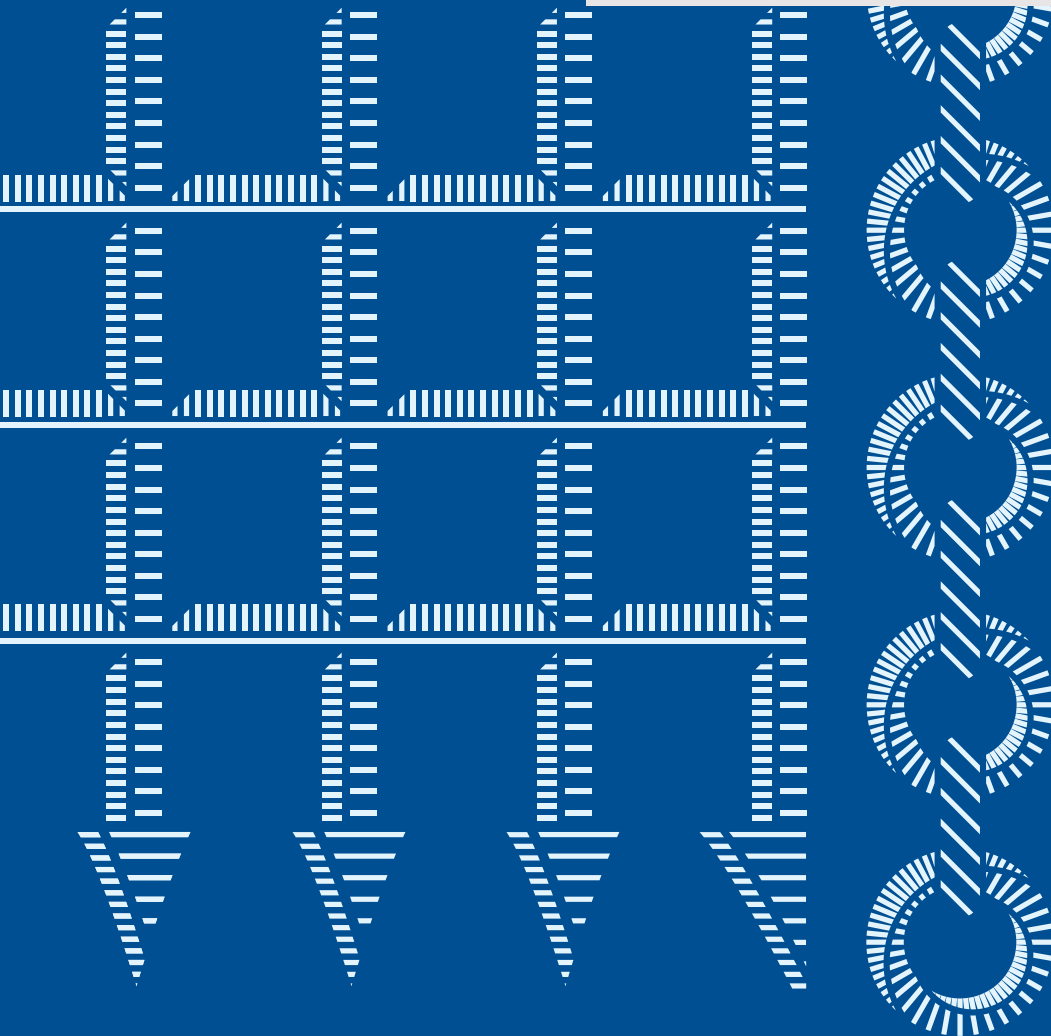
---

# Subsea telecommunications cables: resilience and crisis preparedness

---

First Report of Session 2024–26

HC 723 / HL Paper 179



---

# Joint Committee on the National Security Strategy

The Joint Committee on the National Security Strategy is appointed by the House of Lords and the House of Commons to consider the National Security Strategy.

## Current membership

### House of Lords

[Lord Boateng](#) (Labour; Life peer)

[Baroness Fall](#) (Conservative; Life peer)

[Lord Hutton of Furness](#) (Labour; Life peer)

[Baroness Kidron](#) (Crossbench; Life peer)

[Lord Robathan](#) (Conservative; Life peer)

[Lord Sarfraz](#) (Conservative; Life peer)

[Lord Sedwill](#) (Crossbench; Life peer)

[Lord Tunncliffe](#) (Labour; Life peer)

[Baroness Tyler of Enfield](#) (Liberal Democrat; Life peer)

[Lord Watts](#) (Labour; Life peer)

### House of Commons

[Matt Western](#) (Labour; Warwick and Leamington) (Chair)

[Dame Karen Bradley](#) (Conservative; Staffordshire Moorlands)

[Liam Byrne](#) (Labour; Birmingham Hodge Hill and Solihull North)

[Sarah Champion](#) (Labour; Rotherham)

[Mr Tanmanjeet Singh Dhesi](#) (Labour; Slough)

[Bill Esterson](#) (Labour; Sefton Central)

[Mike Martin](#) (Liberal Democrat; Tunbridge Wells)

[Edward Morello](#) (Liberal Democrat; West Dorset)

[Andy Slaughter](#) (Labour; Hammersmith and Chiswick)

[Emily Thornberry](#) (Labour; Islington South and Finsbury)

[Derek Twigg](#) (Labour; Widnes and Halewood)

[Sir Gavin Williamson](#) (Conservative; Stone, Great Wyrley and Penkridge)

## Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place within the United Kingdom, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chair.

## Publication

This Report, together with formal minutes relating to the report, was Ordered by the House of Commons and the House of Lords, on 15 September 2025, to be printed. It was published on 19 September 2025 by authority of the House of Commons and the House of Lords. © Parliamentary Copyright House of Commons 2025.

This publication may be reproduced under the terms of the Open Parliament Licence, which is published at [www.parliament.uk/copyright](http://www.parliament.uk/copyright).

Committee reports are published on the Committee's website at [www.parliament.uk/jcnss](http://www.parliament.uk/jcnss) and in print by Order of the House.

## Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on the National Security Strategy, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 4043; the Committee's email address is [jcnss@parliament.uk](mailto:jcnss@parliament.uk). You can follow the Committee on X (formerly Twitter) using [@JointCtteNSS](https://twitter.com/JointCtteNSS).

---

# Contents

	<b>Executive summary</b>	<b>1</b>
<b>1</b>	<b>Introduction</b>	<b>4</b>
	Our inquiry	4
<b>2</b>	<b>Overview and trends</b>	<b>5</b>
	Overview	5
	Trends	6
	Business-as-usual resilience	7
<b>3</b>	<b>Threat picture</b>	<b>9</b>
	Strategic context	9
	Security crisis	10
	Should we worry?	11
	Concepts	11
	Sabotage capabilities	12
	Limitations	13
	Implications	14
<b>4</b>	<b>System vulnerabilities</b>	<b>17</b>
	Overview	17
	Concentrated targets	17
	Landing stations	17
	Concentration of data in cables and tipping points	19
	Rerouting without spare capacity	20
	Satellites to the rescue?	21
	Our view of the implications	22

<b>5</b>	<b>Repair vulnerabilities</b>	<b>24</b>
	Repair times	24
	UK capabilities	25
	Navy reservists	26
<b>6</b>	<b>Moderate and catastrophic impacts</b>	<b>28</b>
	Minor and moderate disruption	28
	Outlying islands	28
	Financial sector	28
	Military communications	29
	Catastrophic system failure	30
	Degraded international connectivity	30
	Communications	31
	Supply chains and transport	31
	Financial sector	32
	Emergency services and responses	32
	Government view	33
<b>7</b>	<b>Legal Responses</b>	<b>35</b>
	Overview	35
	What to do?	36
	Novel interpretations	37
	Risks of novel interpretations	39
	Can the UK make a difference?	39
	Strengthening flag state rules	41
	Solutions	42
<b>8</b>	<b>Military and monitoring responses</b>	<b>44</b>
	Monitoring issues	44
	Military activities in peacetime	47
	Deterrence concepts	47
	Atlantic Bastion	53

<b>9 Governance and planning</b>	<b>55</b>
Governance	55
Stakeholder views	57
A joined-up oversight body	57
Crisis responses	58
Spatial planning	60
<b>Conclusions and recommendations</b>	<b>62</b>
<b>Formal minutes</b>	<b>68</b>
<b>Witnesses</b>	<b>70</b>
<b>Published written evidence</b>	<b>72</b>

---

# Executive summary

The UK's internet system relies almost entirely on subsea telecommunications cables to connect to the outside world. These cables carry the data that power our economy, everyday communications and critical services. For many years the UK's internet connection has been based on assumptions about international stability and commercial efficiency. As the geopolitical outlook worsens, now is a good time to take stock of our security and resilience arrangements.

Our inquiry found some things to commend. The UK has plenty of cable routes and good repair processes for business-as-usual breakages. Ministers and officials are working with industry on mitigating risks; schemes to monitor cables are gathering pace and plans to test resilience are maturing. That is all welcome.

But security vulnerabilities abound. There is a limit to how much cables can be protected from adversaries using civilian vessels to 'accidentally' drag anchors over the seabed. There are particular vulnerabilities around the UK's outlying islands, military cables and the financial sector. The trend towards critical amounts of data being concentrated in new high-capacity cables will create a small set of high-value targets.

Onshore infrastructure is a further concern. Cables come ashore via landing stations, which remain vulnerable to unsophisticated sabotage. Many onward terrestrial links converge towards data centres, creating worrying levels of concentration. This all presents risks for low-level deniable attacks which – while not causing national disruption – would be costly, provocative and hard to prevent.

We were disturbed about the level of scepticism we encountered in some parts of industry and government about the value of preparing for more extensive co-ordinated attacks. Some suggested we should focus on fishing accidents or low-level hybrid sabotage. We are not persuaded that this is a good basis for mitigating catastrophic risk: there needs to be a much clearer acceptance about the UK's strategic vulnerability in the event of hostilities.

We agree that severe disruption risks are low, and hype is unhelpful. Extensive damage is not likely outside a period of heightened tension. But given the deteriorating security environment and the UK's growing military

role in Europe, we can no longer rule out the possibility of UK infrastructure being targeted in a crisis. We are also not confident that the UK could prevent such attacks or recover within an acceptable time period.

We accept that individual industry operators have few incentives to advocate costly resilience measures for a crisis that may never come. The Government, by contrast, has a duty to prepare competently for low-likelihood high-impact events. We caution strongly against the Department for Science, Innovation and Technology favouring a 'business as usual' industry view of aggregate national security risk.

We also believe the Government's resilience concept focuses too much on having 'lots of cables' and pays insufficient attention to the system's actual ability to absorb unexpected shocks. We found general uncertainty about how much damage the system can sustain before data stops rerouting properly. We estimate the impacts of data rerouting failures would vary across sectors, ranging from moderate to catastrophic.

The Government cannot achieve complete security, but some changes can help. More muscular deterrence is key. The Government must be prepared to impose genuine costs for state-backed sabotage that go beyond public attribution. Updating the 140 year-old legal framework is essential, alongside integrated monitoring and response systems. Better repair schemes, security upgrades, and more diverse cable routes are needed too. We are calling for:

- A UK-flagged sovereign repair ship to guarantee speedier repairs, alongside live military exercises to practice escorting repair ships in a security crisis;
- A reservist scheme to train personnel on cable repair skills, to be called upon in the event of a crisis;
- Legal changes to introduce tougher penalties for malicious damage, a UK-led international push to test novel legal concepts (for example applying anti-piracy provisions), and an expanded port state control regime;
- New integrated monitoring and alert systems to improve early warning and vessel interception;
- Better impact assessments and contingency plans across key sectors;
- Security upgrades to critical infrastructure sites and systems, alongside emergency 'good enough' repair plans;
- A clearer strategy to diversify cable routes at sea and on land to avoid pinch-points of high-value targets;

- Better governance through a cross-government co-ordination unit to improve join-up, and to address the tension between commercial and security objectives.

---

# 1 Introduction

## Our inquiry

1. The modern internet has largely developed during a period of geopolitical stability, following the end of the Cold War. That world is now fading. The United States is reconsidering its security interests. Revisionist powers are challenging the rules-based international order.<sup>1</sup> Now is a good time to examine some assumptions that underpin our national security.
2. We launched this inquiry in February 2025 to examine the security of the UK's subsea telecommunications cables. We focused in particular on preparedness to deal with incidents during periods of heightened international tension or a time-sensitive security crisis. Our objective was to assess the adequacy of resilience, contingency plans and response options.
3. Subsea cables have been a topic of interest and some unhelpful hype recently. Our Report focuses on issues that may help advance debate or address long-standing challenges. Chapters 2–6 set out the trends, threats, resilience weaknesses and impacts. Chapters 7–9 set out military, legal and governance response options.
4. We considered carefully how much detail on matters of national security is appropriate to place in the public domain, striking a balance between transparency and caution. We are providing the Government with more sensitive details of our assessments at higher levels of classification. We are grateful to all who contributed to our inquiry.

---

1 [Q1](#) [Elisabeth Braw]

---

## 2 Overview and trends

### Overview

5. Subsea telecommunications cables run for thousands of miles across the world, connecting countries in a system that constitutes the backbone of the global internet. These cables are typically run by private businesses and carry everything from financial transactions worth trillions of dollars to WhatsApp messages. Around 570 cables (plus a further 80 planned) carry between 95 and 99% of the world’s intercontinental telecommunications data.<sup>2</sup> Satellites can typically handle only circa 5% of subsea cable data capacity.<sup>3</sup>
6. Subsea cables generally connect to national data infrastructure via landing stations. These are small hubs on the coastline which process and feed the cable data onwards into a country’s terrestrial network. Landing stations are also usually run by private businesses.
7. As an island the UK is almost entirely reliant on subsea cables to transmit the data connecting it to the outside world. JISC, an infrastructure provider, said the UK is “uniquely positioned” among G7 nations in terms of economic size, proximity to Europe and shallow waters access.<sup>4</sup> The UK also acts as a key onward transit route for transatlantic cables: APTelecom, a consultancy, described the UK as a “global hub for internet traffic” and “one of the world’s most important locations”.<sup>5</sup>
8. There is good resilience in the system for business-as-usual situations. Around 64 cables land in the UK, including 45 international systems, as shown in Figure 1. Around 50 of these are thought to be active. There are also cables running through the Channel Tunnel.<sup>6</sup>

---

2 Department for Science, Innovation and Technology ([USC0022](#)), RAND Europe ([USC0035](#)), TeleGeography, [How many submarine cables are there anyway](#), 27 February 2025, [Q60](#) [Sir Chris Bryant]

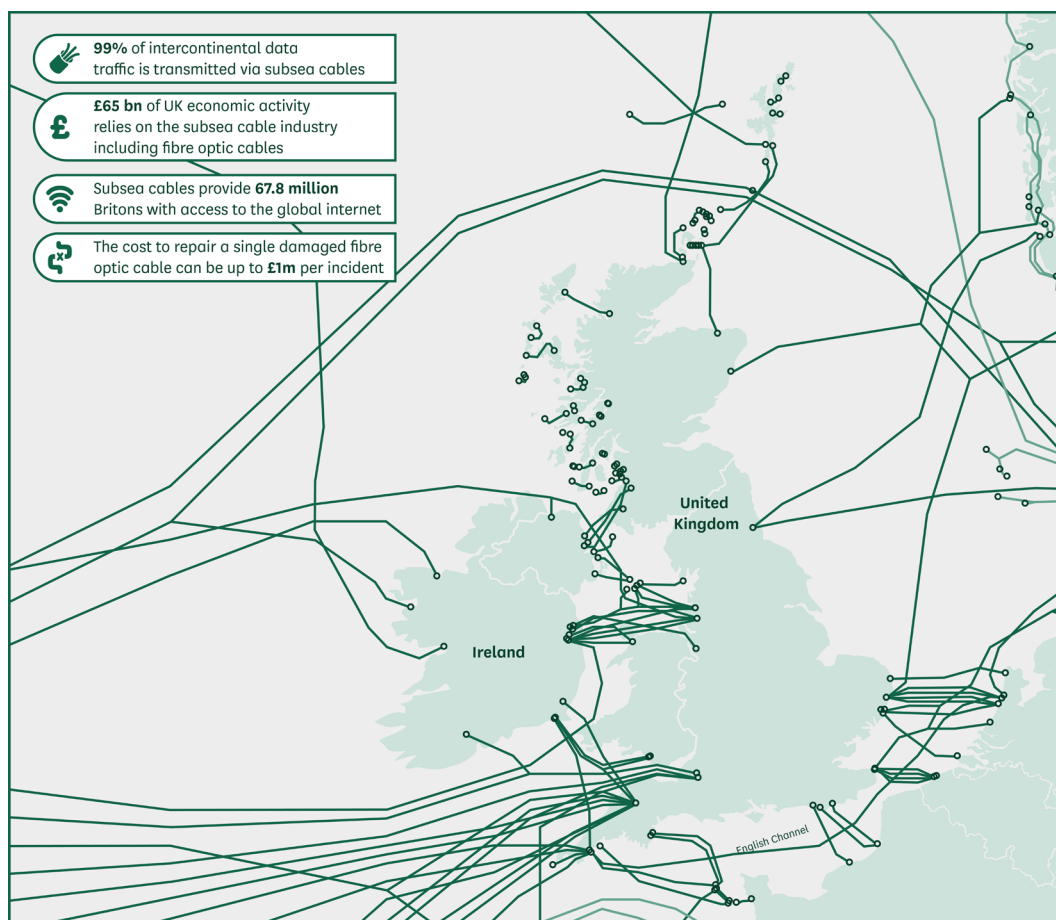
3 Department for Science, Innovation and Technology ([USC0022](#))

4 JISC ([USC0019](#))

5 APTelecom ([USC0027](#))

6 [Q60](#) [Sir Chris Bryant]

**Figure 1: UK connections to undersea cables**



Source: [HM Government, National Security Strategy](#), 2025, p 23

## Trends

9. Demand for cables will increase as data consumption continues to grow rapidly, linked in part to new technologies and AI-based services.<sup>7</sup> A small number of new high-capacity cables are expected to hold a growing proportion of data traffic.<sup>8</sup> Much of this is driven by big tech firms, who are playing an increasingly central role in cable ownership as they seek supply routes for their services.<sup>9</sup> We noted growing concern about the long-term implications for digital competition and strategic reliance if foreign tech firms own a growing proportion of critical internet infrastructure.

7 Ofcom, [Online Nation](#), 2024

8 APTelecom ([USC0027](#)), Vodafone UK ([USC0037](#)), Jeremy Steventon-Barnes ([USC0029](#))

9 The share of global network capacity used by big tech content providers has grown from 10% in 2012 to over 70% in 2022. See Telegeography, [Submarine Cable Map](#), 2023. Examination of the potential long-term implications of big tech dominance of subsea infrastructure were beyond the scope of our inquiry.

10. Dr Sidharth Kaushal, Senior Fellow for Sea Power at the Royal United Services Institute (RUSI), told us that the system would therefore become “both more efficient and more fragile” over the next decade.<sup>10</sup> As APTelecom emphasised, “cutting a newer cable would be far more disruptive than cutting an older one”.<sup>11</sup> These trends are already evident: just two cables account for 75% of the UK’s transatlantic capacity. Both land in Bude, Cornwall.<sup>12</sup>

## Business-as-usual resilience

11. There have been numerous allegations of Russia and China using proxy actors to sabotage subsea cables, particularly in the Baltic and Indo-Pacific regions respectively.<sup>13</sup> Cables can be damaged by vessels dragging heavy equipment over the seabed. The Council on Geostrategy noted that distinguishing genuine accidents from malicious intent remains difficult.<sup>14</sup> However, the European Subsea Cables Association (ESCA) said sabotage is rare and the overwhelming majority of faults are not malicious: 70–80% of cable faults arise from fishing activity or vessels dragging anchors, and 20–30% are caused by other non-malicious factors.<sup>15</sup>
12. We examined the arrangements for fixing damaged cables with Mick McGovern, General Manager of Marine Operations at Alcatel Submarine Networks, and Alasdair Wilkie, Chairman of the Atlantic Cable Maintenance & Repair Agreement. We found the process for handling business-as-usual incidents is efficient, well tested and robust. There are also good systems for internet data to reroute to other cables automatically in the event of damage, and such incidents generally pass unnoticed by internet users.<sup>16</sup>
13. In the absence of a security crisis, the risk of severe disruption to UK connectivity is very low.<sup>17</sup> As Captain (Rtd) Adrian Pearce, formerly of the Royal Navy, put it, isolated events “are a nuisance but unlikely to cause

---

10 [Q3](#)

11 APTelecom ([USC0027](#))

12 Jeremy Steventon-Barnes ([USC0029](#))

13 China Strategic Risks Institute, [Testing the waters: Securing the UK’s subsea cables against grey-zone threats](#) June 2025

14 Council on Geostrategy ([USC0041](#)), RAND Europe ([USC0035](#)), European Subsea Cables Association ([USC0026](#))

15 For example, abrasion, equipment failure or by natural hazards such as seafloor currents, storms, submarine landslides, or sediment flows. See European Subsea Cables Association ([USC0026](#))

16 [Qq47-56](#)

17 [Q4](#) [Matthew Bowden], [Q18](#) [Commodore (Rtd) John Aitken], [Q32](#) [Laura Catterick], European Subsea Cables Association ([USC0026](#)), Chatham House ([USC0045](#)), Captain Adrian Pierce RN (Rtd) ([USC0050](#))

strategic issues”.<sup>18</sup> The most likely scenario for intentional disruption involves a persistent low-level threat or occasional sabotage.<sup>19</sup> Sir Chris Bryant MP, then Minister for Data Protection and Telecoms,<sup>20</sup> told us that the UK is “quite well practised at making sure that we are resilient and can respond quickly” to business-as-usual breakages.<sup>21</sup>

#### 14.

##### **CONCLUSION**

The UK’s strategic reliance on subsea cables will likely continue for the foreseeable future. The cable industry provides a commendable and commercially efficient repair service, which ensures good resilience against moderate damage. We do not believe there is an imminent threat to the UK’s national connectivity.

---

18 Captain Adrian Pierce RN (Rtd) ([USC0050](#)). See also [Q4](#) [Matthew Bowden], [Q18](#) [Commodore (Rtd) John Aitken], [Q32](#) [Laura Catterick], European Subsea Cables Association ([USC0026](#)), Chatham House ([USC0045](#))

19 Centre for Peace and Security, Coventry University ([USC0008](#))

20 The relevant ministers changed roles before the publication of this Report. On first mention they are cited as “the then Minister”. Subsequent mentions refer only to “the Minister” for ease, noting that our Report cites their evidence in relation to their capacity at the time.

21 [Q60](#)

---

## 3 Threat picture

### Strategic context

15. The 2025 National Security Strategy argues that “For the first time in many years, we have to actively prepare for the possibility of the UK homeland coming under direct threat, potentially in a wartime scenario”.<sup>22</sup> Russia is the biggest near-term concern. Russia has lost significant manpower and equipment in the Ukraine conflict; assessments of its ability to reconstitute its forces range from two to ten years.<sup>23</sup> NATO’s Secretary General, Mark Rutte, recently estimated that Russia would be “ready to use military force against NATO within five years”.<sup>24</sup>
16. Full-scale armed conflict remains unlikely. But lower-level aggressive activities during a period of heightened tension, or shaping operations ahead of limited confrontation, are no longer unthinkable.<sup>25</sup>
17. Sir David Omand GCB, former Director of GCHQ and UK Security and Intelligence Co-Ordinator, warned that the UK “will be right in the crosshairs after a [Ukraine] ceasefire and that we really must expect the Russians to pick on us”.<sup>26</sup> These concerns have gained particular salience given US ambivalence to European security, the UK’s support for Ukraine, and UK leadership of security groups outside NATO structures.<sup>27</sup> Experts also warn of low-level incidents leading to unintended escalation.<sup>28</sup>

---

22 Cabinet Office, [National Security Strategy](#), 2025. European defence spending is also growing amid concerns over a US drawdown, though the International Institute of Strategic Studies notes that the emphasis on GDP spending “masks actual capabilities, contributions, sustainability and effectiveness”. See IISS, [Global defence spending soars to new high](#), 12 February 2025

23 International Institute of Strategic Studies, [Russia’s Information Confrontation Doctrine in Practice \(2014–Present\): Intent, Evolution and Implications](#), 2025; IISS, [Defending Europe without the United States](#), 15 May 2025, p 8. Norway estimated 2–3 years, Denmark estimated 2–5 years, the UK Chief of Defence Staff estimated 5–10 years.

24 Chatham House, [NATO chief warns Russia could use military force](#), 9 June 2025

25 RAND Europe (USC0035); IISS, [Defending Europe without the United States](#), 15 May 2025. We note in particular the situation in Ukraine, Russia’s increasingly militarised commercial and societal structures, and history of opportunistic aggression.

26 Oral evidence taken on 30 April 2025, [Q10](#) [Sir David Omand]

27 Oral evidence taken on 30 April 2025, [Q10](#) [Sir David Omand]

28 CEPA, [Up North: Confronting Arctic Insecurity Implications for the United States and NATO](#), 5 December 2024

## Security crisis

18. The National Risk Register 2025 sets out a reasonable worst-case scenario involving damage to the UK's internet connectivity. This provides the public-facing basis for contingency planning. It notes that repairing cables can take weeks but concludes that adequate connectivity would resume within hours as data is speedily rerouted via other cables.<sup>29</sup>
19. However, its assessments only envisage a loss of transatlantic cables. For reasons we have struggled to discern, it does not explore what would happen if the critical onward connections to Europe are also disrupted in a co-ordinated attack.<sup>30</sup> This matters because, as the next chapter sets out, the impacts on connectivity would be much more serious. We therefore explored whether this scenario should be given more consideration.

### Box 1: Threat actors

- **Russia** is currently the primary threat actor capable of causing severe national disruption to the UK, owing to its geographical proximity, strategic culture, capability mix and willingness to use military force and proxies to achieve political objectives.
- **China** possesses an increasingly capable array of maritime assets, though its primary security focus remains on the Indo-Pacific and its current ability to project power in the Euro-Atlantic at pace during a security crisis is more limited. In the event of UK involvement in an Indo-Pacific security crisis, however, we would not rule out some targeting of UK assets.
- **Non-state actors** might also cause some disruption, as demonstrated in 2024 when subsea cables in the Red Sea were damaged amid Houthi attacks on shipping. A further incident in September 2025 affected Microsoft's Azure cloud services, sparking further concern. Wider extremist groups might also target some cables or landing stations. As autonomous underwater vehicles become more commercially available, new concerns may arise around terrorist or extreme direct-action organisations seeking to disrupt parts of the economy.

Sources: Department for Science, Innovation and Technology ([USC0022](#)), RAND Europe ([USC0035](#)), Chatham House ([USC0045](#)), Council on Geostrategy ([USC0041](#)), Professor Timothy Edmunds and Professor Andrew Neal ([USC0018](#)), BBC, [Microsoft cloud services disrupted by Red Sea Cable cuts](#), 7 September 2025

29 HM Government, [National Risk Register](#), 2025, p 60

30 [Q60](#)

## Should we worry?

20. We found many in the cable industry were more concerned about fishing accidents than future geopolitical crises. For example, Peter Jamieson, an industry expert (writing in a personal capacity), told us:

There is a heightened sense of awareness regarding malicious actions, potentially Russian, due to recent incidents in the Baltic but there is no clear evidence of any intent ... Government should first tackle the biggest threat to subsea cables, commercial fishing, then anchors ... Address those threats, then we can focus on the perceived threat from Russia.<sup>31</sup>

21. Alex Towers, Director of Policy and Public Affairs at BT Group, said that it was “hard to imagine” how a large proportion of the system infrastructure could be degraded. He accepted that the industry was “less well prepared” for a “concerted and co-ordinated attack”, but maintained this:

seems a very distant prospect from where we are today and what we know about everything from the past hundred years’ worth of protecting this infrastructure.<sup>32</sup>

22. The ESCA said that recent concerns about “a rising number of incidents/threats to subsea telecommunications cables ... is not borne out in the data” and warned against “premature speculation” about suspected sabotage incidents. It acknowledged that “different considerations” would apply in a security crisis but cautioned against “excessive security-focused restrictions” to recent concerns.<sup>33</sup>

23. In our evidence session the Minister for Data Protection and Telecoms, Sir Chris Bryant MP, said the Government had “robust” contingency plans. He suggested that, by examining the possibility and consequences of a co-ordinated attack, we were focusing on “apocalyptic” scenarios and “overegging this pudding”.<sup>34</sup>

## Concepts

24. There is however good evidence suggesting that, in a worsening security environment, the current absence of a crisis is not a strong argument for deprioritising defensive preparations as a deterrent.<sup>35</sup> Russian military

---

31 Peter Jamieson ([USC002](#))

32 [Q32](#)

33 European Subsea Cables Association ([USC0029](#))

34 [Q57](#)

35 RAND Europe ([USC0035](#)), Chatham House ([USC0045](#)), Captain Adrian Pierce RN (Rtd) ([USC0050](#)), Council on Geostrategy ([USC0041](#))

concepts on the targeting of critical infrastructure are well documented.<sup>36</sup> Key tenets include inflicting calibrated levels of damage to hold adversaries at risk in a security crisis, and eroding military and economic resources to coerce an adversary to de-escalate on acceptable terms.<sup>37</sup>

25. Subsea cables are likely to feature prominently in such thinking, given their centrality to financial and communications systems.<sup>38</sup> Witnesses stressed that they can be damaged without lethal force, often without military assets, and below the threshold of armed conflict.<sup>39</sup> Russia has been pursuing wider measures to reduce the impacts of economic shocks and isolation.<sup>40</sup>

## Sabotage capabilities

26. Dr Kaushal told us that Russia’s capabilities are substantial but not infinite. They are broadly split between the Main Directorate for Deep Sea Research (known as the GUGI) and the Russian Navy.<sup>41</sup> The GUGI operates titanium-hulled vessels such as the Losharik which can target cables at extreme depth. Longer voyages require motherships (for example the Belgorod) for support.<sup>42</sup> Russia is also thought to use ‘commercial’ vessels for reconnaissance.<sup>43</sup>
27. Elisabeth Braw, Senior Research Fellow at the Atlantic Council, emphasised that Russia “is quite willing and able to recruit freelancers” for unsophisticated activities like anchor-dragging.<sup>44</sup> Some maritime experts envisage a gradual bifurcation of the shipping industry as so-called

---

36 Benjamin Schmitt, Alan Riley, Michał Kurtyka, [Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond](#), May 2025

37 Michael Kofman et al, Center for Naval Analysis, [Russian military strategy: core tenets and operational concepts](#), 2021; Michael Kofman et al, Center for Naval Analysis, [Russian strategy for escalation management, evolution of key concepts](#), 2020

38 Council on Geostrategy (USC0041); RUSI, [Stalking the seabed](#), 25 May 2023; RUSI, [How might the Kremlin test NATO’s collective defence?](#), 3 January 2025

39 Qq5–6 [Elisabeth Braw, Dr Sidharth Kaushal]. See also European Parliament, [Security threats to subsea communications cables and infrastructure](#), 2022; Professor Aurel Sari, [Protecting maritime infrastructure from hybrid threats](#), Hybrid CoE Research Report 14, 2025

40 CSIS, [Down but not out: The Russian economy under Western sanctions](#), 11 April 2025.

See also Russia’s overland connectivity options: Submarine Cable Networks, [The Eurasia Terrestrial Cable Network](#)

41 [Q6](#)

42 RUSI, [Stalking the seabed](#), 25 May 2023

43 Politico, [Russia uses civilian boats to spy in the North Sea, joint report says](#), 19 April 2023

44 [Q6](#)

‘grey fleets’ seek to evade Western sanctions<sup>45</sup>—which may gradually institutionalise and enlarge the pool of vessels that could be enlisted for deniable activity.<sup>46</sup>

28. Proxy actors can also be used for sabotaging onshore internet infrastructure (discussed in the next chapter).<sup>47</sup> The Russian intelligence services have repeatedly demonstrated capabilities to penetrate protected sites directly and via hired help.<sup>48</sup>
29. We considered the credibility of more ambitious offensive options, including pre-positioning explosive charges on cables or their repeaters,<sup>49</sup> and deploying specialist divers. Professor Kevin Rowlands, Head of the Royal Navy’s Strategic Studies Centre (but appearing in a personal capacity) told us that this would be “difficult and risky” due to the impacts of weather, seabed floor movement, currents and detection potential.<sup>50</sup> We further explored eavesdropping risks: experts told us undetected cable tampering is difficult underwater.<sup>51</sup>

## Limitations

30. As we set out in subsequent chapters, there are many mitigations: monitoring schemes are increasing, and NATO would track subsurface activity closely in a crisis. Would-be saboteurs may be identified by the security services. Infrastructure operators are experienced in repairs, and landing stations can be rebuilt given sufficient time.<sup>52</sup>
31. There are also limits to Russia’s capabilities. Matthew Bowden, Director and General Manager at Red Penguin Marine, a subsea engineering firm, told us cables are hard to pinpoint and anchor dragging is not guaranteed to work

---

45 Lloyds List, [Shipping splits into ‘parallel universes’ as global trade continues to decouple](#), 17 October 2024

46 Carnegie Endowment, [The Baltic Sea at a Boil: Connecting the Shadow Fleet and Episodes of Subsea Infrastructure Sabotage](#), 5 June 2025

47 Secret Intelligence Service, [Speech by Sir Richard Moore, Chief of SIS](#), 29 November 2024; Mark Galeotti, [Gangsters at war](#), November 2024

48 For example the arson attack on a London warehouse in March 2024, incendiary devices which ignited at a Birmingham depot, and numerous incidents across Europe. See BBC, [Why small-time criminals burned a London warehouse for Russia’s mercenary group Wagner](#), 8 July 2025; The Guardian, [Photos of Birmingham DHL fire suggest device could have downed plane](#), 10 December 2024

49 Repeaters are specialised pieces of equipment that strengthen the signal over long distances.

50 [Q8](#)

51 [Q49](#) [Mick McGovern]

52 Vodafone Group ([USC0037](#)); APTelecom ([USC0027](#))

first time.<sup>53</sup> Dr Kaushal noted Russia has limited numbers of motherships, extreme depth vessels and experienced personnel. Operational readiness is another factor—a fire in 2019 on the Losharik resulted in years of repairs.<sup>54</sup>

32. The transit time between cable locations, alongside diving time for targeting deep sea cables, also limits the scale, speed and deniability of an operation. Commodore (Rtd) John Aitken, former Deputy Director of Submarines in the Royal Navy, told us that destroying large numbers of cables simultaneously would be “extremely difficult”.<sup>55</sup> Professor Rowlands noted that advances in autonomous underwater vehicles might change this calculation, particularly if cheap versions enable one-way missions.<sup>56</sup> Commodore Aitken noted however that there were currently limitations around battery life, sensing and range.<sup>57</sup>
33. A key factor limiting the likelihood of extensive attacks is intent—mounting a successful effort would be hard, and would probably be part of a wider suite of hostile acts in a security crisis. However, the lack of intent today does not guarantee future security: Russian calculations about the merits of targeting the UK are likely be influenced by extraneous factors and can change faster than resilience measures can be upgraded—as shown by previous military incursions and sabotage.<sup>58</sup> There is also evidence that Russia is conducting preparatory reconnaissance useful to sabotage: Windward AI reports increased anomalous loitering over sensitive sites for UK infrastructure, and the Yantar surveillance vessel has conducted numerous operations.<sup>59</sup>

## Implications

34. Overall this suggests that Russia has the concepts, capabilities and preparatory intent for conducting sabotage if necessary. Substantial damage could be achieved below the threshold of armed conflict. A sophisticated operation including onshore targets would be needed to cause national disruption. This would likely need to include the onward subsea connections to Europe. The evidence suggests however that these connections (excepting the Channel Tunnel) are vulnerable: as Commodore Aitken put it, “we should not consider them safe”.<sup>60</sup>

---

53 [Q9](#)

54 See HI Sutton, [Naval News](#) (2021)

55 [Q17](#)

56 See HI Sutton, [Naval News](#) (2021)

57 [Q14](#)

58 For example Georgia in 2008, Ukraine in 2014 and 2024, alongside sabotage efforts across Europe.

59 Windward AI ([USCO021](#)), China Strategic Risks Institute, [Testing the waters: Securing the UK's subsea cables against grey-zone threats](#) June 2025

60 [Q18](#)

35. We therefore disagree with the Minister’s statements on the risk. We do not believe this view reflects the balance of evidence, or the assessments in the Strategic Defence Review about the “immediate and pressing” threat from Russia, and the National Security Strategy’s conclusion that whole-of-government preparations for a “direct threat” to the homeland are necessary.<sup>61</sup> Some parts of Government are sufficiently concerned so as to procure nuclear-capable F-35A aircraft, missile defence systems and assemble Home Defence plans.<sup>62</sup> And while the UK may not be facing an immediate crisis today, the past 25 years show that strategic surprises do happen.<sup>63</sup>

36. We subsequently questioned the then Chancellor of the Duchy of Lancaster, Rt Hon Pat McFadden MP, about the Minister for Data Protection and Telecom’s position. The Chancellor of the Duchy of Lancaster said he was “not here to criticise another Minister” but agreed that we “cannot proceed on the basis of the same assumptions that we would have had some years ago”.<sup>64</sup> The Minister for Data Protection and Telecoms subsequently wrote to us confirming that he took “the threat of a coordinated attack extremely seriously” and outlined preparations for “severe” disruption arising from a hybrid attack.<sup>65</sup>

37. **CONCLUSION**

The Government’s resilience assessments must take greater account of the worsening security environment over the next 5–10 years. The National Security Strategy and Strategic Defence Review set out serious preparations for future crises. However, the Minister for Data Protection and Telecoms suggested that exploring the risks of a co-ordinated attack on subsea infrastructure was unhelpfully “apocalyptic”. We disagree. Focusing on fishing accidents and low-level sabotage is no longer good enough. The UK faces a strategic vulnerability in the event of hostilities. Publicly signalling tougher defensive preparations is vital, and may reduce the likelihood of adversaries mounting a sabotage effort in the first place.

---

61 Cabinet Office, [National Security Strategy](#), 24 June 2025

62 HM Government, [Strategic Defence Review](#), 2025; HM Government, [UK to purchase F-35As and join NATO nuclear mission as Government steps up national security and delivers defence dividend](#), 24 June 2025

63 We noted the limited forewarning in many of these, for example 9/11 and subsequent conflicts in the Middle East, the 2008 financial crash, Russia’s 2014 invasion of Crimea, the Covid-19 pandemic, and Russia’s 2022 invasion of Ukraine.

64 Oral evidence taken on 14 July 2025, [Q23](#) [Pat McFadden]

65 Letter from the Minister for Data Protection and Telecoms to the Chair relating to subsea cables, [15 August 2025](#)

38.

**CONCLUSION**

We also found sceptical views in some parts of the cable industry about the risks of co-ordinated attacks. We agree that resilience across the sector is generally robust, major disruption is unlikely, and hype is unhelpful. But we caution against adopting ‘business as usual’ industry views to determine national security risk: individual operators have few financial incentives to prepare for a crisis that may never come. The Government, by contrast, has a duty to prepare competently for low-likelihood, high-risk scenarios. The lessons of 9/11, the financial crash, Covid-19 pandemic and the war in Ukraine are reminders that such events do happen.

39.

**RECOMMENDATION**

The Government should update its public and private risk scenarios to cover extensive co-ordinated sabotage to subsea and terrestrial internet infrastructure, including onward connections to Europe.

---

## 4 System vulnerabilities

### Overview

40. Throughout our inquiry we encountered a general perception that the UK is not likely to face severe disruption even in the face of a concerted malicious effort, because having lots of cables provides sufficient resilience. As the Minister for Data Protection and Telecoms put it:

We are slightly overegging this pudding, if you do not mind me saying. We have 64 subsea cables, which is a higher number than islands of our size would normally have, 50 of which are active. There are vulnerabilities, but I do not want to exaggerate.<sup>66</sup>

41. Our review suggested a more mixed picture: good resilience against moderate incidents but also widespread security vulnerabilities and uncertainty about how much damage the system can withstand.

### Concentrated targets

42. Many cables cluster in a few locations around the UK and Ireland. A vessel journeying from Land's End towards Aberystwyth would cross around 20 cables. Another ship travelling down the Suffolk coastline would cross eight major cables in just a few hours.<sup>67</sup>

### Landing stations

43. Landing stations may be the most vulnerable part of the system. Many locations house multiple cables—for example, Lowestoft has five, and Bude has nine.<sup>68</sup> Physical security across sites varies. Some could be rendered inoperable by sabotage.<sup>69</sup> Cyberattacks are a further worry. The terrestrial links between the subsea cable, the landing station and the data centres can also be sabotaged with unsophisticated tools.<sup>70</sup>

---

66 [Q60](#)

67 TeleGeography, [Submarine cable map: United Kingdom](#) (accessed 8 August 2025)

68 TeleGeography, [Submarine cable map: United Kingdom](#) (accessed 8 August 2025)

69 [Q43](#)

70 [Q10](#) [Matthew Bowden], [Q43](#) [Alex Towers]

44. The other end of cables can also be targeted. Sabotaging landing stations on the European coastline for example would achieve similar effects, with added complications around co-ordinating repairs across multiple countries.<sup>71</sup> (There are also high security cables elsewhere. We are providing the Government with further assessments of this and other vulnerabilities in private).
45. Some improvements are expected. The National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC) audited some landing sites last year, and one “major” site owner is upgrading security.<sup>72</sup> The Minister for Data Protection and Telecoms told us landing stations had been designated Critical National Infrastructure (CNI).<sup>73</sup> The new Resilience Action Plan has ambitions for new CNI standards by 2030. The European Union is also calling for security improvements.<sup>74</sup>
46. Vodafone Group noted that the funnelling of terrestrial cables to datacentres remains a concern.<sup>75</sup> Professor Adam Beaumont, Chairman of telecoms company AQL Holdings, highlighted the potential for “catastrophic” attack vectors if high-concentration locations are targeted.<sup>76</sup> Chief Constable Gavin Stephens, Chair, National Police Chiefs’ Council, said the police were not currently resourced to protect extensive numbers of sensitive locations in a security crisis and would require support—potentially under the Home Defence Programme cited in the Strategic Defence Review.<sup>77</sup>

47. **CONCLUSION**

Many cable landing stations are vulnerable to attack. The Government and operators must take the risk of state-backed sabotage seriously, including against targets in Europe.

---

71 RAND, [Subsea cables are vulnerable to sabotage](#), 8 July 2025

72 Letter from the Minister for Data Protection and Telecoms, regarding undersea cables, [10 July 2025](#)

73 [Q59](#), Letter from the Minister for Data Protection and Telecoms, regarding undersea cables, [10 July 2025](#)

74 Cabinet Office, [UK government resilience action plan](#), 14 July 2025; European Commission, [Commission and the High Representative present strong actions to enhance security of submarine cables](#), 21 February 2025

75 Vodafone Group ([USC0037](#))

76 Professor Adam Beaumont ([USC0006](#)).

77 [Qq37–41](#); HM Government, [Strategic Defence Review](#), 2025, p.89

**48. RECOMMENDATION**

The National Protective Security Authority (NPSA) and National Cyber Security Centre should require all UK landing stations to be target-hardened to sufficient levels to deter state-backed sabotage. They should require landing station operators to develop within 12 months an emergency ‘good enough’ repair plan to recover from co-ordinated attacks. The NPSA should also conduct a similar exercise with European counterparts for relevant landing stations on the continent.

**49. RECOMMENDATION**

To help mitigate risks around the clustering of high value targets, the Government should encourage subsea cable providers to connect to landing stations, terrestrial routes and data centres outside high-concentration points.

## Concentration of data in cables and tipping points

- 50.** The UK’s resilience against major disruption relies on data from severed cables rerouting swiftly via intact cables. We encountered uncertainty about how much damage the system could sustain before that process stops working properly. Mr Wilkie suggested “an awful lot”.<sup>78</sup> Mr Bowden cautioned that we should not get “sidetracked” by the number of cables cut:

It is the capacity of the cables that are cut, and the information that is being passed over them, that is important, as well as the ability to reroute ... It is not quite as simple as just saying, ‘We have had six out of our 11 cables cut. Everyone, light your hair on fire and run around in small circles’.<sup>79</sup>

- 51.** Jeremy Steventon-Barnes, former Chief Technology & Information Officer at EXA Infrastructure, provided us with estimated cable capacity between the UK, the US and Europe. We compared this against other sources. Two transatlantic cables carry around 75% of capacity, and seven cables might carry around 93% of capacity. This does not mean 75–93% of UK internet activity would collapse if these cables were severed: not all data travels via subsea cables (plenty remains within the UK) and the figures suggest the UK’s European links have sufficient capacity to absorb all of the affected data—accounting for the fact that those cables are unlikely to be running at 100% capacity.<sup>80</sup>

---

78 [Q48](#)

79 [Q4](#)

80 Jeremy Steventon-Barnes ([USC0029](#)); TeleGeography, [Submarine cable 101](#), 2025

52. But the data also suggest that critical amounts of UK-Europe capacity are concentrated in a relatively small number of cables and landing stations.<sup>81</sup> A large proportion of Europe’s direct transatlantic capacity is also concentrated in a few cables, which could be targeted. Mr Steventon-Barnes concluded that:

at a whole European level, it must be recognised that transatlantic capacity is concentrated across a relatively small number of cables, presenting a significant risk of total loss of connectivity in the event of a coordinated attack by a hostile state actor.<sup>82</sup>

53. We further noted that the amount of spare capacity will be lower than the headline figures suggest, as these typically refer to theoretical potential rather than the immediately available live (or ‘lit’) capacity.<sup>83</sup> Mr Steventon-Barnes suggested that not all fibres will be using the equipment needed to operate at maximum capacity.

## Rerouting without spare capacity

54. An incident in July 2025 provided a small local case study on rerouting issues, when the cable connecting Orkney and Banff was damaged. The BBC reported that OpenReach delivers the broadband connection to the islands, while access to data packages is sold by separate businesses (such as Vodafone or PlusNet). Some customers experienced no disruption, others had data rerouted via other routes after a little while, while others faced more extensive problems.<sup>84</sup>
55. We were uncertain how well the data rerouting system would work at a national level in a crisis involving severely degraded international connectivity. However, the indications are not auspicious. The system involves a vast array of actors, automated protocols and different levels of visibility across data traffic.<sup>85</sup> It is managed by disparate set of private sector businesses and commercial contracts: some manual intervention is possible but there is no central co-ordinating intelligent brain monitoring

---

81 APTelecom ([USC0027](#))

82 Jeremy Steventon-Barnes ([USC0029](#))

83 TeleGeography, [Submarine cable 101](#), 2025; Jeremy Steventon-Barnes, supplementary submission ([USC0055](#))

84 BBC, [Cable damage disrupts internet services in Orkney and Shetland](#), 26 July 2025; BBC, [Orkney and Shetland internet cable ‘fixed by next weekend’](#), 27 July 2025

85 Some of the lessons from the 2024 Red Sea incident are instructive. See for example Noction, [Navigating undersea cable disruptions](#), February 2024; Telegeography, [The Red Sea](#), 17 January 2024; Subsea cables, [Invisible infrastructure, visible chaos](#), August 2025. For system complexity see Microsoft, [Advancing global network reliability through intelligent software—part 2 of 2](#), 16 November 2020

the type or destination of data, or overall network health.<sup>86</sup> This stands in contrast to the energy grid, overseen by the National Energy System Operator.<sup>87</sup>

56. Kevin Adams, Deputy Director for Telecoms Security and Resilience at the Department for Science, Innovation and Technology (DSIT), assured us that the Government had developed an emergency response plan including “how we would prioritise traffic, repair and so on”.<sup>88</sup> This appeared to relate to the Government’s reasonable-worst-case scenario of transatlantic disruption. We queried the likelihood of identifying and prioritising data for critical services at sufficient pace in a more severe crisis. Mr Towers of BT indicated the difficulties, and suggested:

It would be a different world to the one we have traditionally lived in, where everything is treated equally ... in terms of traffic, but it is a question worth considering.<sup>89</sup>

## Satellites to the rescue?

57. The UK’s strategic reliance on cables looks set to continue for the foreseeable future—alternative satellite connectivity can only handle around 5% of subsea cable capacity.<sup>90</sup> Starion UK, a space engineering firm, suggested the growth in commercial satellites over the next decade might provide a limited “backstop” in a crisis.<sup>91</sup> NATO’s project HEIST is also exploring rerouting via satellites if cables are attacked.<sup>92</sup>
58. Professor Sir Martin Sweeting of the Surrey Space Centre, University of Surrey, outlined options across geostationary orbit satellites, low earth orbit constellations, high altitude platforms and free-space optical communications.<sup>93</sup> The evidence we received suggests there is some value, but the options all have limitations around availability, cost, speed

---

86 See previous reference; [Q50](#).

87 NESO, [What we do](#) (Accessed 4 September 2025)

88 [Qq58–60](#)

89 [Q33](#)

90 Professor Sir Martin Sweeting ([USC0051](#)), Department for Science, Innovation and Technology ([USC0022](#))

91 Professor Adam Beaumont (Chairman at aql) ([USC0006](#)), Starion UK Ltd ([USC0028](#))

92 NATO, [NATO-funded project to reroute internet to space in case of disruption to critical infrastructure](#), 28 August 2024

93 Professor Sir Martin Sweeting ([USC0051](#))

and capacity.<sup>94</sup> At a national level, APTelecom concluded satellites are “incapable of delivering data in the necessary volumes” barring a “major generational breakthrough”.<sup>95</sup>

## Our view of the implications

59. The evidence therefore suggests that the UK has sufficient resilience to make an immediate wholesale disconnection from the internet implausible. But a tipping point scenario does appear possible, where data rerouting stops working properly because the capacity of onward routes is too limited. We have chosen not to publish our estimates on key targets for taking this critical amount of capacity offline.<sup>96</sup>
60. We questioned the Minister for Data Protection and Telecoms about these concerns. He informed us that it was “a moot point about how we recognise things in the risk register”—a contention we struggled to follow, given its centrality to contingency planning.<sup>97</sup> He further argued that severing most or all of the transatlantic cables would alone be “quite an ask and, I would argue, an unlikely scenario to be basing our risk on”.<sup>98</sup>
61. We pressed for details as to why contingency plans did not account for disruption to European connections. Mr Adams of DSIT told us there were “good reasons” why the Government has focused only on “transatlantic cables as a reasonable worst-case scenario”, including the “resilience in our connectivity to Europe” and cables in the Channel Tunnel.<sup>99</sup>

62. **CONCLUSION**

The Government’s resilience concept focuses too much on ‘having lots of cables’. This pays insufficient attention to the network’s actual capacity to absorb shocks and does not account for onshore vulnerabilities and long-term trends towards a more brittle system. There is also limited understanding of much damage the system can sustain before data stops rerouting properly, triggering temporary systemic connectivity failure. This does not appear to feature as a serious consideration in the Government’s contingency planning.

---

94 For example emergency communications, or microwave-based links to outlying islands. See Professor Sir Martin Sweeting ([USC0051](#)); Starion UK Ltd ([USC0028](#)); APTelecom ([USC0027](#)); Archangel Lightworks Ltd ([USC0015](#))

95 APTelecom ([USC0027](#))

96 We are providing some further details to the Government in private.

97 See for example [Q34](#) [Laura Catterick]

98 [Q58](#)

99 [Q58](#)

**63.**

**RECOMMENDATION**

The Government's resilience plans should focus in more detail on the level of immediately available capacity in the cable system during a security crisis. The Department for Science, Innovation and Technology should request operators to provide regular updates on the scale and type of data each cable carries, short notice rerouting capacity and their ability to prioritise critical services. It should further develop detailed contingency plans for rerouting data through the Channel Tunnel, including in scenarios where high-concentration terrestrial routes are temporarily disabled.

---

## 5 Repair vulnerabilities

### Repair times

64. Repairing damaged cables is not very quick. Alasdair Wilkie of ACMA told us that repair ships would leave port within 24 hours of being notified of a cable fault and might travel at around 12 knots. Repairs nearby, for example in the Irish Sea, may involve up to two days’ travel time and five days’ repair time, whereas transit to the mid-Atlantic might take seven days plus ten days for repairing a cable. Bad weather could increase this to a month.<sup>100</sup>
65. The two main cable maintenance and repair consortiums—ACMA and the Atlantic Private Maintenance Agreement (APMA)—have three repair vessels each, and could each field two vessels covering the North Atlantic region.<sup>101</sup> Mr Wilkie said the available inventory enabled ACMA vessels to carry out “between 10 and 20 repairs per cable system”.<sup>102</sup> The cable industry also works to universal jointing standards which might enable interoperable support across other vessels and equipment.<sup>103</sup> Matthew Bowden, Director and General Manager at Red Penguin Marine, emphasised however that each ship could only focus on one break at a time:
- You will have to wait until a cable ship becomes free. At that point, when you start racking up additional cable breaks ... your repair capability can be used up quite quickly.<sup>104</sup>
66. Repair timelines also depend on ships being in the vicinity and willing to travel in the face of possible hybrid maritime aggression, such as ‘accidental’ collisions. Mr Wilkie confirmed repair vessels probably would not put to sea in a conflict zone without a military escort.<sup>105</sup>

---

100 [Q48](#)

101 [Q47](#)

102 [Q53](#) [Alasdair Wilkie]

103 See for example SubConnect, [UK/UQJ products and services](#) (accessed 11 September 2025)

104 [Q4](#) [Matthew Bowden]

105 [Q53](#)

## UK capabilities

67. We queried the Government’s influence over which repairs are prioritised in a crisis. Mr Wilkie explained that cable owners and repair outfits “will talk to each other and decide” on priorities.<sup>106</sup> The Government told us that it would try to play some role through plans developed by its subsea cables incident response working group.<sup>107</sup> Mr Bowden noted:

We do not have any UK-owned repair capability. Global Marine, which was a UK company, has just been bought by Singapore.<sup>108</sup> What are the ramifications of that? Orange Marine runs the vessel out of Brest. Global Marine runs the one out of Curaçao at the moment.

With the greatest respect to our French allies ... I would bet quite a lot of money that the French Government would influence Orange Marine in terms of their prioritisation, and it would not necessarily be in our favour.<sup>109</sup>

68. The Government might try to requisition a UK-flagged ship, though only if it is still operational. ACMA’s UK-based CS Sovereign was built in 1991 and many repair ships have an average lifespan of 35–40 years, indicating that it will retire sometime around 2030.<sup>110</sup> Industry analysts suggest there is little redundant repair capacity that could be purchased at short notice on the open market—cable maintenance ships are expensive to run, and tend to operate with minimal downtime.<sup>111</sup>
69. The European Subsea Cables Association (ESCA) and Vodafone said the Government should consider developing a sovereign repair capability.<sup>112</sup> The USA offers one model; it has invested in sovereign repair capability in the form of the Cable Security Fleet.<sup>113</sup> This has been operated by SubCom, a private contractor, for an annual sum of US\$10 million. In return, the US

---

106 [Q48](#) [Alasdair Wilkie]

107 [Q60](#) [Kevin Adams]

108 The deal involved Keppel Infrastructure Fund, headquartered in Singapore, and a co-investor. See Keppel, [Keppel’s flagship infrastructure fund leads acquisition of subsea cable specialist Global Marine Group](#), 10 March 2025

109 [Q8](#) [Matthew Bowden]. Orange Marine is a wholly-owned subsidiary of Orange Group, the largest shareholder of which is the French state. Orange Marine [Who we are](#) (accessed 23 July 2025); Financial Times, [French telcos explore carve-up of Patrick Drahi’s SFR](#), 14 July 2025

110 Global Marine, [C.S. Sovereign Data Sheet](#), 2018; Infra-Analytics and Telegeography, [The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies](#), June 2025

111 Data Centre Dynamics, [The cable ship capacity crunch](#), 6 December 2022

112 European Subsea Cables Association ([USCO026](#)); Vodafone ([USCO037](#))

113 Sophia Besch and Erik Brown, [Securing Europe’s Subsea Data Cables](#), Carnegie Endowment, December 2024, p.5

government received continuous access to “two US-flagged and crewed cable ships ... which are required to be available for laying, maintaining, and repairing critical cables”.<sup>114</sup>

70. The European Commission has proposed an EU Cable Vessels Reserve Fleet, possibly funded via a public-private partnership.<sup>115</sup> A recent report recommended contracting repair services on the market in the short term, alongside strategic stockpiling of equipment in “high-risk areas”, ahead of eventually acquiring the reserve fleet.<sup>116</sup>

71. **CONCLUSION**

The UK needs more confidence in access to cable repair vessels: the current fleet is ageing, and erstwhile UK businesses have been acquired by foreign entities.

72. **RECOMMENDATION**

The Government should acquire a genuinely sovereign cable repair ship by 2030. This could be leased to industry on favourable terms during peacetime and made available for Government use in a crisis. The Government should set out a timetable for this in response to this Report.

## Navy reservists

73. We heard that procuring a repair ship would not be a quick fix. Mr Wilkie noted that “repair ships take about three years to build, and the staff to man them about ten years to train”.<sup>117</sup> The ESCA recommended “training naval reservists on jointing, cable handling, and other functions and skills that may be needed for cable repair or deployment” as a way of building capacity.<sup>118</sup> John Wrottesley, Executive Director of the ESCA, said this would need to be done properly:

---

114 CSIS, [Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition](#), August 2024

115 European Commission, [Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security](#), 21 February 2025; Bloomberg, [EU in Talks to Fund Fleet to Repair Damaged Subsea Cables](#), 15 February 2025

116 European Commission, [Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security](#), 21 February 2025, 4.2, pp.13–14

117 [Q54](#) [Alasdair Wilkie]

118 European Subsea Cables Association ([USC0026](#))

If there was co-operation or a public/private partnership, and if naval reservists were the solution, that would have to involve having them integrated into the repair ecosystem, because you do not want to lose those skills and that knowledge over time if people just come and train, and then leave. They have to be part of that ecosystem.<sup>119</sup>

74. This would align with the Strategic Defence Review’s ambitions to make better use of reservists.<sup>120</sup> The then Minister for the Armed Forces agreed that:

We need more zig-zag careers, where people operating in uniform in a regular capacity move to a reserve capacity or an industrial capacity and then move back into a regular capacity ... That helps make us more resilient.<sup>121</sup>

75. **RECOMMENDATION**

The Royal Navy should establish a cadre of reservists and serving personnel to learn cable repair skills on commercial repair vessels. These could be called on in periods of heightened tension.

---

119 [Q54](#) [John Wrottesley]

120 HM Government, [Strategic Defence Review](#), 2025, p.65

121 [Q67](#) [Luke Pollard]

---

## 6 Moderate and catastrophic impacts

- 76.** We explored the potential impacts of disruption in order to determine what sorts of private and public sector contingency measures are proportionate. The first part of this chapter covers minor and moderate damage to particularly vulnerable areas. This might be caused by state actors in a period of heightened political tension, or by non-state actors, proxies or direct action groups seeking to cause economic, societal or military disruption. The second part examines catastrophic system failure caused by extensive co-ordinated attacks in a security crisis or prelude to conflict.

### Minor and moderate disruption

#### Outlying islands

- 77.** The UK's outlying islands are served by a small number of cables, suggesting scope for localised sabotage which might assume outsized political importance in the context of a security crisis.<sup>122</sup> In 2022 for example the cables connecting the Shetland Islands were accidentally severed by a fishing vessel. Local media reported widespread card payment failures, alongside disruption to mobile and landline services.<sup>123</sup> In July 2025 the cable connecting Orkney and Banff was damaged. Hundreds of customers were affected, the Balfour Hospital switchboard went down (though 999 calls were unaffected) and some businesses said internet-based systems did not work for days.<sup>124</sup>

#### Financial sector

- 78.** High-frequency trading and many other financial services rely on subsea cables, with \$1.5 trillion in cross-border trading (23% of the world's total) travelling through subsea cables every day.<sup>125</sup> The loss of key low latency

---

122 [Q1](#) [Matthew Bowden]

123 BBC, [Damaged cable leaves Shetland cut off from mainland](#), 20 October 2022

124 BBC, [Cable damage disrupts internet services in Orkney and Shetland](#), 27 July 2025; Shetland News, [Lerwick post office 'stranded' with no internet and poor 4G signal](#), 6 August 2025

125 Department for Science, Innovation and Technology ([USC0022](#))

transatlantic connections, plus damage to back-up routes, could cause significant disruption and competitive disadvantage.<sup>126</sup> Wider disruption to transatlantic cables would cause even more problems. The Minister for Data Protection and Telecoms said:

if all or a substantial proportion of the transatlantic cables were cut, or two of the most significant ones ... that would lead to very significant disruption to the internet, to all the essential services, to data services and to financial transactions. There would be very substantial disruption to the state ...

[However] even if you were to cut off all the transatlantic cables there would be disruption for some period, but it would reroute fairly quickly, within a matter of hours.<sup>127</sup>

79. UK Finance, an industry body, said financial services generally have good resilience against moderate disruption, and some firms have data rerouting plans. Resilience regulations provide further contingency frameworks, and there has been some scenario testing through the Cross Market Operational Resilience Group (for example a 2024 power outage exercise).<sup>128</sup>

## Military communications

80. The UK reportedly operates secure cables for military and intelligence communications. Damage would be undesirable, particularly in a period of heightened tension. Dr Sidharth Kaushal, Senior Fellow for Sea Power at RUSI, told us these systems had limited redundancy compared to commercial networks. Commodore (Rtd) Aitken told us there were back-up options, though these might take time to come online and operate with lower functionality.<sup>129</sup>

81. **CONCLUSION**

The UK has particular vulnerabilities around outlying islands, the financial sector and military communications cables. These should be a key focus for contingency planning.

---

126 Lloyd's Market Association ([USC0042](#)), Vodafone Group ([USC0037](#))

127 [Q60](#)

128 UK Finance ([USC0053](#))

129 [Q5](#), [Q17](#)

# Catastrophic system failure

## Degraded international connectivity

- 82.** The European Subsea Cables Association said that there is strong resilience in the system, but cautioned that prolonged or widespread outages would lead to:

economic losses, operational delays, and challenges for critical national infrastructure ... it could negatively impact many sectors including financial markets, international trade and logistics, energy supply and distribution.<sup>130</sup>

- 83.** The evidence in Chapter 4 suggests that national connectivity disruption is worth considering. We found few specifics on how this might unfold for a country with the UK's stature and data-heavy economy. There are various precedents, including small islands and regional failures.<sup>131</sup> But as Professor Adam Beaumont, Chairman of AQL Holdings noted, small islands rely on external data centres whereas the UK has substantial domestic data centre infrastructure.<sup>132</sup> Ukraine offers other lessons, though it conversely has extensive resilience pathways and an unusually low concentration of choke points.<sup>133</sup>

- 84.** A key problem might arise from data rerouting failures affecting access to the international Domain Name System (DNS). Cloudflare, a tech firm, describes DNS as the “phonebook of the internet”, which tells devices where an internet domain name is located.<sup>134</sup> Telecommunications experts note that interruptions to the DNS or border gateway patrol can create cascading functionality failures.<sup>135</sup> The importance of DNS was illustrated in 2021, when Facebook and all of its subsidiary sites went down due to a technical glitch affecting DNS access.<sup>136</sup>

---

130 ESCA ([USC0026](#))

131 For example cable breaks affecting Tonga, Matsu, and various regional blackouts and deliberate shutdowns. See [Q4](#) [Elisabeth Braw]; BBC, [Tonga volcano: Internet restored five weeks after eruption](#), 22 February 2022. Ukraine has also experienced some regional challenges.

132 Professor Adam Beaumont (Chairman at aql) ([USC0006](#)). Around 79% of the UK's top 1000 websites have some form of local access, according to the Internet Society, which also suggests immediate connectivity collapse is unlikely. See Internet Society, [United Kingdom](#), 2024

133 Cloudflare, [One year of war in Ukraine: Internet trends, attacks, and resilience](#), February 2023; Cloudflare, [Tracking shifts in Internet connectivity in Kherson, Ukraine](#), 2022

134 Cloudflare, [What is DNS?](#) (accessed 14 August 2025)

135 Bronwyn Howell, [Beyond Infrastructure: Internet Ecosystem Resilience and the Public Good](#), 29 May 2025

136 The Guardian, [Facebook outage: what went wrong and why did it take so long to fix after social platform went down](#), 5 October 2021

- 85.** Alex Towers, Director of Policy and Public Affairs at BT Group, suggested that severe cable disruption would affect UK access to sites using international domains (such as .com or .eu) quickly, whereas .uk sites would be less affected. Some locally stored data would provide temporary functionality, but he thought “it would not take a huge amount of time for .uk to start encountering problems” too if DNS access is severely degraded.<sup>137</sup>
- 86.** Many .uk sites also use international security authentication protocols, plugins, payment systems, updates and other services which could break.<sup>138</sup> Jeremy Steventon-Barnes, former Chief Technology & Information Officer at EXA Infrastructure, argued that the complex interdependencies across internet services could create “cascades of failures which may result in extended outages even once underlying network connectivity has been restored”.<sup>139</sup>

## Communications

- 87.** International mobile communications would likely be degraded quickly,<sup>140</sup> whereas domestic communications would probably face few issues in the first instance.<sup>141</sup> Lloyds Market Association suggested that “a severe disruption to subsea cables might lead to widespread internet and phone signal blackouts”.<sup>142</sup> There is some precedent for regional failures: in 2012 a fibre optic cable connecting the North West Highlands, Skye and the Western Isles was damaged. Local media reported that “phone lines, broadband and cash machines were all affected. 999 calls could not be made”.<sup>143</sup> During the 2022 Shetland Island incident, both mobile and landline services were disrupted.<sup>144</sup>

## Supply chains and transport

- 88.** Wider disruption to transport and supply chains is possible if just-in-time logistics are disrupted by payment or system authentication failures, which in turn could affect fuel or food deliveries.<sup>145</sup> Any spillover to airport systems

---

137 [Qq32-33](#)

138 Infosec, [Third-party authentication](#), July 2022

139 Supplementary submission from Jeremy Steventon-Barnes ([USC0055](#))

140 [Q2](#) [Matthew Bowden]

141 Landline services are gradually switching to Voice over Internet Protocol systems, which might cause complications. The data traffic would presumably remain within the UK and may be less liable to immediate disruption.

142 Lloyd’s Market Association ([USC0042](#))

143 West Word, [Community newsletter](#), June 2012

144 BBC, [Damaged cable leaves Shetland cut off from mainland](#), 20 October 2022

145 [Q1](#) [Matthew Bowden], Vodafone Group ([USC0037](#)), Oluwakemi Adeyanju ([USC0009](#)), Lloyd’s Market Association ([USC0042](#)). For assessments of food supply chain see National Preparedness Commission, [Just in case](#), 2025

could cause extensive disruption: as a point of comparison, an air traffic control incident in August 2023 affected 700,000 passengers and cost airlines and consumers around £100 million.<sup>146</sup>

## Financial sector

- 89.** Laura Catterick, Director of Resilience and Cyber at UK Finance, told us that catastrophic disruption to the UK’s financial sector as a result of cable damage was a largely untested, “highly unlikely” but high-impact scenario. She said there is no “sector view” of financial services’ overall reliance on cables: “we do not know whether there are choke points, vulnerable cables or more important cables”. Ms Catterick also outlined potential access failures to international financial networks.<sup>147</sup> There would be follow-on consequences for financial stability.
- 90.** Some card payment systems have offline backup functionality, though it is unclear how well this would work if they are affected by a protracted internet outage.<sup>148</sup> Mr Steventon-Barnes suggested UK payment providers could be asked to use more resilient infrastructure.<sup>149</sup> This might build on plans set out recently by the Bank of Finland for offline card payment systems to boost resilience.<sup>150</sup> UK Finance called for co-ordination forums and a cross-sector prioritisation matrix for severe disruption scenario planning.<sup>151</sup>

## Emergency services and responses

- 91.** Mr Towers of BT Group told us that the 999 system had “quite a lot of contingency and resilience built into it” and that there is no reliance on international connections. We heard that emergency services communications would still function, and that local resilience forums would support responses—drawing on experiences from the Mighty Oak national power outage exercises.<sup>152</sup>

---

146 Financial Times, [UK air traffic control failure cost up to £100mn, finds review](#), 14 November 2024

147 [Q34](#)

148 Wallester, [Credit card offline processing](#), 7 August 2024. There were 18.3 billion contactless payments across the UK in 2023. By 2033 just 6% of adults are expected to pay in cash. See UK Finance, [UK payment markets summary](#), July 2024

149 Supplementary submission from Jeremy Steventon-Barnes ([USC0055](#))

150 Other Nordic countries are exploring similar moves. Reuters, [Exclusive: Nordics and Estonia rolling out offline card payment back-up in case internet cut](#), 7 May 2025

151 UK Finance ([USC0053](#))

152 [Q31](#) [Gavin Stephens]

- 92.** Chief Constable Gavin Stephens, Chair of the National Police Chiefs’ Council, said they had reviewed 68 national police systems and found seven which did not have legal agreements ensuring UK-based data access.<sup>153</sup> Domestic connectivity issues might temporarily affect digital evidence retrieval, but overall he was confident that on-the-ground policing would be resilient.<sup>154</sup>
- 93.** Dr Fenella Wrigley MBE, Chief Medical Officer and Deputy CEO at London Ambulance Service, and Ambulance Medical Advisor at NHS England, told us that “key NHS systems are all UK-based”—including care records, the NHS app, NHS login, clinical systems and computer-aided ambulance dispatch.<sup>155</sup>
- 94.** Dr Wrigley highlighted a risk that degraded internet speeds could create glitches affecting access to emergency services’ patient notes. Dr Wrigley told us that control rooms and responders could revert to paper alternatives.<sup>156</sup> Communications could also revert to radio if needed, and crews could handle a regional internet failure by using hailing channels to liaise with other services.<sup>157</sup>

## Government view

- 95.** We found limited public detail on plans to handle the cascading effects of cross-sector internet disruption at a national level. This stands in contrast to areas such as energy grid failure.<sup>158</sup> Kevin Adams, Deputy Director for Telecoms Security and Resilience at the Department for Science, Innovation and Technology (DSIT) assured us that DSIT had recently developed a “national emergency plan”. He explained that individual government departments were then responsible for more “detailed response planning ... for their sectors”.<sup>159</sup>
- 96.** We noted that the Lead Government Department model has been criticised in the past, including by our predecessor Committee, for limited oversight and lack of accountability on whether departments are actually prioritising resilience plans.<sup>160</sup>

---

153 [Q31](#)

154 [Q31](#)

155 [Q35](#)

156 [Qq32–35](#)

157 [Q40](#)

158 See for example some of the details in Department for Energy Security and Net Zero, [National emergency plan 2023](#), July 2023

159 [Qq60–61](#)

160 Letter from the predecessor Committee to the Deputy Prime Minister and Chancellor of the Duchy of Lancaster regarding resilience, [14 June 2023](#)

97. We pressed the Minister for Data Protection and Telecoms for details on the adequacy of these sector-specific responses, given the apparent absence of joined-up plans for the UK’s multi-billion-pound financial services sector. He maintained that “we are pretty well co-ordinated”.<sup>161</sup> He subsequently wrote to us on 15 August stating that DSIT was “working with HM Treasury and the financial sector” to update assessments and HM Treasury “will consider the findings of this updated assessment to inform its policy work on incident preparedness and response”.<sup>162</sup>

98. **CONCLUSION**

The impacts of catastrophic disruption from a co-ordinated attack remain speculative, but are almost certainly highly damaging. We estimate they would include payment and supply chain failures, some degraded communications, overstretched emergency responses, and unexpected cascading issues—all at a time of crisis. We are not convinced there are currently adequate sector-by-sector assessments of reliance on subsea cables, or sufficiently detailed plans for handling cascading consequences if data rerouting stops working properly. We are pleased the Government is starting to address this, with a particular focus on the finance sector.

99. **RECOMMENDATION**

The Department for Science, Innovation and Technology should ensure all lead departments have detailed sector-by-sector technical impact studies on areas most likely to be affected and response plans—notably finance, maritime and air traffic, communications, defence and supply chains including food and fuel. We suggest such assessments are handled securely given their value to hostile actors. We note that some cascading impacts may not be immediately obvious—it may therefore be helpful to begin with an underpinning assessment of internet failure modes and how this would affect critical systems. The Cabinet Office resilience teams could usefully help to co-ordinate and audit these assessments.

100. **RECOMMENDATION**

Emergency services should ensure their business continuity plans highlight any areas of critical reliance on foreign internet servers, and account for temporary internet disruption in the event of a security crisis.

---

161 [Qq60-61](#)

162 Letter from Minister for Data Protection and Telecoms to the Chair regarding subsea cables, [15 August 2025](#)

---

# 7 Legal Responses

## Overview

- 101.** Deterring and punishing malicious activity is crucial—but there are few legal provisions to interdict, investigate and penalise those who damage cables, unless the incident occurs within a state’s territorial waters.<sup>163</sup> Professor Aurel Sari, Professor of Public International Law at the University of Exeter, and Fellow of Supreme Headquarters Allied Powers Europe, emphasised that sabotage can easily occur outside the areas where relevant jurisdiction applies and that “this gap in the law presents a vulnerability that hostile actors may be tempted to exploit”.<sup>164</sup> The International Law Association (ILA) concluded that:

there are limited grounds in the [United Nations Convention on the Law of the Sea] to undertake enforcement measures against private vessels suspected of committing acts of damage to submarine cables and pipelines in all maritime spaces.<sup>165</sup>

- 102.** The UN Convention on the Law of the Sea (UNCLOS) provides the key framework for international maritime law, supplemented by various other agreements.<sup>166</sup> We heard that changing UNCLOS itself is probably a very long-term and difficult goal.<sup>167</sup> But smaller changes to national legislation can help. The Minister for Armed Forces, Luke Pollard MP, indicated that some updates could feature in the forthcoming Defence Readiness Bill.<sup>168</sup> Mr Adams of DSIT told us that the Government would therefore be:

---

163 That is, within 12 nautical miles or circa 22 kilometres of the baseline. [Q24](#) (Professor Aurel Sari). See Annex 1 for further notes. This section concerns the legal options available to states. Private cable owners may also seek to take crews of suspect vessels to court, though there are also various legal difficulties. See [Virgin Media Ltd v Joseph Whelan t/a M & J Fish](#) [2017] EWHC 1380 Admlty.

164 Professor Aurel Sari, [Protecting maritime infrastructure from hybrid threats](#), Hybrid CoE Research Report 14, 2025, p.23

165 In relation to states other than the flag state of the suspect vessel. See International Law Association (ILA), [Submarine Cables and Pipelines under International Law, Interim Report](#) (2020) para 183(b); [United Nations Convention on the Law of the Sea](#), 10 December 1982

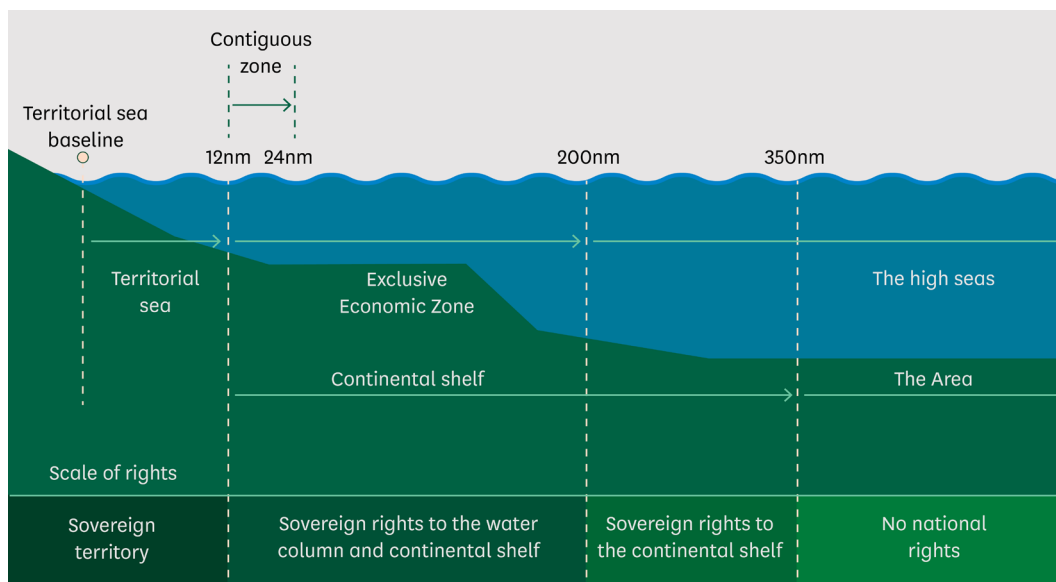
166 [Q26](#); [United Nations Convention on the Law of the Sea](#), 10 December 1982

167 [Qq 24–25](#)

168 [Q64](#); HM Government, [Strategic Defence Review](#), 2025, Ch 6, para 12, p.90

looking at the full raft of legislation to see what powers might need updating in terms of the role and responsibilities of industry in relation to the cables, the powers around data sharing and the use of technology on these cables, as well as powers during an emergency.<sup>169</sup>

**Figure 2: Maritime jurisdictional zones and coastal states' legal rights**



Source: Environmental Audit Committee, Fourteenth Report of Session 2017–19, [Sustainable Seas](#), HC 980; courtesy of the Royal Society, [Future Ocean Resources: metal rich minerals and genetics evidence pack](#), 2017

## What to do?

- 103.** The UK has various laws around telecommunications infrastructure, sabotage and maritime activity.<sup>170</sup> The Submarine Telegraph Act 1885 is the foundational piece of legislation in cable security. It specified a penalty of £100 for damaging a cable by culpable negligence.<sup>171</sup> The fines have been raised slightly since, though we noted the deterrence value was probably quite small. Modest further increases are possible via secondary legislation. The Minister for Data Protection and Telecoms said that they could increase fines to several thousand pounds but that, ultimately, wider upgrading of the legislation is needed.<sup>172</sup>

169 [Q64](#) [Kevin Adams]

170 For example the [Telecommunications \(Security\) Act 2021](#), the [National Security Act 2023](#), the [Merchant Shipping Act 1995](#), and the [Continental Shelf Act 1964](#)

171 [Submarine Telegraph Act 1885](#) 3(2). The penalty for wilful cable damage is up to two years' imprisonment or an equivalent fine. Note that proof of intent can be difficult to establish. The Act has been generally interpreted as applying only within the territorial waters of the UK and British Overseas Territories. See Professor Jacques Hartmann ([USC0040](#))

172 [Q64](#)

- 104.** Tougher criminal liability provisions might also help. Professor Jacques Hartmann, Professor of International Law and Human Rights at the University of Dundee, called on the Government to explicitly “clarify that damage to subsea cables constitutes a criminal offence”—whether through updates to the 1885 Act, the Criminal Damage Act 1971, or new legislation.<sup>173</sup> He noted this would be consistent with the UK’s obligation under UNCLOS Article 113.<sup>174</sup>

## Novel interpretations

- 105.** International frameworks still place considerable limits on state jurisdiction for incidents further away from the shore. We therefore considered the merits and risks of some more novel concepts to extend UK jurisdiction or apply new penalties.<sup>175</sup>

## Expanding jurisdictional application

- 106.** The ILA notes that the 1884 Convention for the Protection of Submarine Telegraph Cables “confers primary jurisdiction on the State of registration of the offending vessel and secondary jurisdiction to the state of citizenship of the offender”.<sup>176</sup> Professor Hartmann notes that Article 10 of the Convention does include provisions for a warship or other specially commissioned ship to board a foreign-flagged vessel suspected of cable damage on the high seas, in order to require the ship’s master to produce the ship’s papers and to take statements from the ship’s officers.<sup>177</sup> These may then be used as evidence in legal proceedings in the vessel’s flag state.

---

173 Professor Jacques Hartmann ([USC0040](#)); [Q28](#) [Professor Aurel Sari]

174 This says that states should criminalise damage to subsea cables and pipelines caused by “by a ship flying its flag or by a person subject to its jurisdiction.” [United Nations Convention on the Law of the Sea](#), 10 December 1982, Art 113; Professor Jacques Hartmann (Professor of International Law and Human Rights at University of Dundee) ([USC0040](#))

175 International Law Association has produced a detailed analysis of various legal options for the protection of subsea cables. These are summarised in International Law Association, [Submarine Cables and Pipelines under international law \[Third\] Interim Report](#), 2024.

176 See International Law Association, [Submarine Cables and Pipelines under International Law, Interim Report](#), 2020, para 78; and [Submarine Telegraphs Convention](#), 14 March 1884, Article VIII.

177 This provision does not appear to be used very often. Professor Hartmann cites a sole example when an unarmed US navy party boarded a Soviet trawler in 1959. See Professor Hartmann ([USC0040](#))

- 107.** The International Law Commission has previously highlighted considerations around the “protective principle”, which refers to:

the jurisdiction that a State may exercise with respect to persons, property or acts abroad which constitute a threat to the fundamental national interests of a State, such as a foreign threat to the national security of a State.<sup>178</sup>

This might offer some grounds for attempting to apply provisions in the Submarine Telegraph Act 1885, or other legislation covering criminal damage, to incidents further afield.<sup>179</sup> But it is unlikely to be straightforward. There is legal uncertainty around whether enforcement of domestic criminal law could be applied to foreign crew and vessels. UNCLOS Article 73(1) for example specifies enforcement rights in relation to the conservation and management of “living resources”, which may not apply explicitly to subsea cables.<sup>180</sup> The International Law Association notes that:

there appear to be no examples of States served by that cable or pipeline that have adopted national legislation explicitly criminalizing acts of damage to submarine cables and pipelines outside of their territorial waters by foreign vessels or foreign nationals.<sup>181</sup>

## Piracy

- 108.** Professor Hartmann suggested looking at the piracy provisions in UNCLOS Article 101.<sup>182</sup> Piracy provisions helpfully cover the High Seas, where other jurisdiction is weak. But using this concept would also be difficult: piracy typically applies to damage committed by private actors, not states. Professor Sari noted that:

---

178 International Law Commission, “Extraterritorial Jurisdiction”, Annex E, [Report of the work of the fifty-eighth session](#), A/61/10, 2006, para 13

179 See suggestions from Professor Jacques Hartmann ([USC0040](#)). Professor Sari also suggests that in cases of suspected damage to underwater infrastructure, the enforcement of domestic legislation over foreign vessels and their crews within a state’s territorial waters may not be explicitly prohibited by UNCLOS Article 27. See Professor Aurel Sari, [Protecting maritime infrastructure from hybrid threats](#), Hybrid CoE Research Report 14, 2025, p.18

180 See [United Nations Convention on the Law of the Sea](#), 1982, Article 73(1)). See also Professor Aurel Sari, [Protecting maritime infrastructure from hybrid threats](#), Hybrid CoE Research Report 14, 2025, p.24; and International Law Association, [Submarine Cables and Pipelines under international law \[Third\] Interim Report](#), 2024, para 65

181 International Law Association, [Submarine Cables and Pipelines under international law \[Third\] Interim Report](#), 2024, para 89

182 Professor Jacques Hartmann ([USC0040](#)). UNCLOS defines piracy as: “any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed (i) on the high seas, against another ship or aircraft, or against persons or property on board such

You cannot say in the same breath that this [sabotage] is potentially attributable to a state and also to piracy, because they are mutually exclusive categories.<sup>183</sup>

- 109.** Nevertheless, given that it can be difficult to prove a state link—and a ship’s crew are unlikely to admit they are operating on behalf of a foreign intelligence service—the prosecution of responsible individuals as private citizens might provide some deterrent. There may be a need for changes to domestic legislation if this option is pursued.<sup>184</sup>

## Risks of novel interpretations

- 110.** Applying novel interpretations of international law carries risks of retaliation. Dr Marie Jacobsson, former Principal Legal Adviser to the Swedish Ministry for Foreign Affairs, warned about the downsides of seeking “creeping jurisdiction”, and emphasised caution and pragmatism:

There is one thing that every state should have in mind when dealing with this: it is a question of reciprocity. Our own vessels are likely to be subject to the same acts that we perform on other state vessels. That is important.<sup>185</sup>

- 111.** Setting new precedents in international law might also have impacts beyond the maritime sphere.<sup>186</sup> Professor Sari argued that any changes would need to reflect wider “balance of interests” and cautioned:

If a state goes around beating its chest, as it were, about compliance with the rules-based international order but then takes shortcuts, inevitably you will get a charge of hypocrisy and double standards that then tends to stick.<sup>187</sup>

## Can the UK make a difference?

- 112.** We noted that changing international conventions can be difficult, but the UK may be well placed to lead such work. Professor Hartmann argued that, when it comes to strengthening the international legal framework on

---

ship or aircraft; (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State.” ([United Nations Convention on the Law of the Sea](#), 10 December 1982, Art 101)

183 [Q25](#) [Professor Aurel Sari]

184 [United Nations Convention on the Law of the Sea](#), 10 December 1982, Art 105

185 [Q25](#) [Dr Marie Jacobsson]

186 For example, some analysts suggest the Chinese government has used the protective principle to apply various legislation extraterritorially. Alyssa Resar, [“Self-Protection in World Society: Reformulating the Protective Principle in International Law”](#), *Yale Law Journal*, 2025

187 [Qq26–30](#) [Professor Aurel Sari]

cable damage, the UK is “uniquely positioned to lead these efforts on the international stage”.<sup>188</sup> The UK is a signatory to key conventions,<sup>189</sup> and hosts organisations such as the International Maritime Organization (IMO), the headquarters of the International Law Association (ILA), and the London Maritime Arbitrators Association.<sup>190</sup> London is reportedly a global centre for maritime and transport dispute resolution too.<sup>191</sup>

**113. CONCLUSION**

The legal provisions for responding to malicious cable damage are weak. It is encouraging that the Government has identified the forthcoming Defence Readiness Bill as a potential legislative vehicle to implement changes. We would like to emphasise the urgency of making progress internationally too: legal developments can be slow, and the matter is pressing. The UK should use its strong credentials in order play a leading international role on this topic.

**114. RECOMMENDATION**

The Government’s review of legislation must pay particular attention to strong deterrents, such as major fines and criminal liability, that can be applied to private actors suspected of working for or on behalf of foreign states.

**115. RECOMMENDATION**

The Government should explore new options for taking a more robust approach to interdicting suspicious vessels—for example applying piracy provisions to cables that land in the UK or seeking a limited extension of domestic criminal law jurisdiction. It should commission a legal opinion on options and risks, and publish this within six months for consultation with industry and international partners. The Government should, however, remain cautious about the risks of reciprocal action from adversaries and we do not endorse any particular option at this stage.

---

188 Professor Jacques Hartmann ([USCO040](#))

189 [Submarine Telegraph Convention](#), 1884; [United Nations Convention on the Law of the Sea](#), 1982; Paris MoU, [Organisation](#) (accessed 2 September 2025)

190 IMO [Contact Us](#) (accessed 2 September 2025); [ILA | WELCOME](#) (accessed 2 September 2025); [LMAA - The Worldwide Leaders In Commercial Maritime Dispute Resolution](#) (accessed 2 September 2025)

191 HFW, [The maritime arbitration universe in numbers: is London’s crown under threat?](#), September 2023

## Strengthening flag state rules

- 116.** Outside coastal state waters, the primary responsibility for enforcing international maritime regulations lies with a vessel’s flag state (that is, where the ship is “registered”).<sup>192</sup> Data from the International Maritime Organisation suggest a substantial rise in vessels using fraudulent flags.<sup>193</sup> Many are thought to be involved in the so-called “shadow fleet”, used by Russia and others for transporting sanctioned oil.<sup>194</sup> The Nordic-Baltic 8++ Group of countries, to which the UK belongs, has promised “appropriate action within international law”.<sup>195</sup>
- 117.** But even legitimately flagged vessels cause problems, as some flag states’ oversight is weak and their enforcement is limited.<sup>196</sup> A 2023 paper for the European Parliament noted the absence of binding international frameworks to regulate registration practices “incentivises companies to register their ships in such countries”.<sup>197</sup>
- 118.** Dealing with powerful countries like China is particularly difficult, as the case of the Chinese-flagged vessel Yi Peng 3 illustrates. The vessel dragged its anchor for 330 kilometres in the Baltic Sea in November 2024, damaging two subsea telecommunications cables.<sup>198</sup> The Chinese government allowed Swedish authorities to board to carry out limited observations, subject to tight restrictions.<sup>199</sup> The Swedish Accident Investigation Board was unable to conclude whether the cable damage had been deliberate or accidental because of:

---

192 [United Nations Convention on the Law of the Sea](#), 10 December 1982, Art 92(1)

193 Lloyd’s List, [Fake flag investigation prompts IMO data review](#), 29 July 2025

194 Lloyd’s List, [Baltic shadow fleet stand off continues as Russia warns of tanker ‘raids’](#), 5 August 2025

195 FCDO, [NB8++ joint statement on the shadow fleet](#), 20 June 2025.

196 Professor Jacques Hartmann (USC0040); Chinese Strategic Risks Institute, [Testing the waters: Securing the UK’s subsea cables against grey-zone threats](#), June 2025, p.29. Both the Paris Memorandum secretariat and the International Chamber of Shipping produces annual performance tables for flag states. See Paris MoU, [WGB Flag performance list 2024](#), July 2025; International Chamber of Shipping, [Shipping Industry Flag State Performance Table 2024/2025](#), 2025

197 EU Parliamentary Research Service, [Addressing ship reflagging to avoid sanctions](#), March 2023

198 Statens haverikommission, [SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3](#), 15 April 2025. Translation from the original Swedish via Google Translate.

199 According to the official Swedish report, the Swedish observers worked under the supervision of their Chinese counterparts. The Swedish prosecutor was not allowed on board. China did not permit a criminal investigation to take place on board, grant access to footage from the vessel’s onboard cameras, or allow interviews with crew to be recorded. The boarding took place over a month after the incident, with the consequence that voyage data from the Yi Peng 3’s Simplified Voyage Data Recorder (S-VDR) had been

the limitations of the investigative measures. [...] Further investigations at an earlier stage on board the vessel would have been necessary to establish what had occurred on board.<sup>200</sup>

## Solutions

- 119.** Applying more joined-up diplomatic pressure on flag states is one option, particular for those flag states that are members of the International Maritime Organization. Dr Jacobsson argued that if a single state tried to apply such pressure, it would likely be ineffective, but that if states were to do so as part of a concerted effort they would stand a better chance of succeeding.<sup>201</sup>
- 120.** Tightening flag state controls is another. This might involve making more progress on work requiring a genuine link between flag state and ownership.<sup>202</sup> However, some industry experts note that governments have been attempting to do this since the 1980s with limited success.<sup>203</sup>
- 121.** Dr Jacobsson suggested making “much more of the International Maritime Organization [IMO], for example, when it comes to flag state responsibilities and how we should interpret maritime security and safety. That is a definite possibility”.<sup>204</sup> This could involve further action around port state control processes.<sup>205</sup> The IMO has encouraged strengthening this regime,<sup>206</sup> which involves:

the inspection of foreign ships in national ports to verify that the condition of the ship and its equipment comply with the requirements of international regulations and that the ship is manned and operated in compliance with these rules.<sup>207</sup>

---

overwritten. Statens haverikommission, [SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3](#), 15 April 2025. Translation from the original Swedish via Google Translate.

200 Statens haverikommission, [SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3](#), 15 April 2025. Translation from the original Swedish via Google Translate.

201 [Q26](#) [Dr Marie Jacobsson]

202 [Q26](#) [Dr Marie Jacobsson]; Professor Jacques Hartmann ([USC0040](#))

203 Oral evidence taken by the House of Lords International Relations and Defence Committee on 24 November 2021, [Q81](#) [Professor Anna Petrig]

204 [Q29](#) [Dr Marie Jacobsson]

205 [Q25](#) [Dr Marie Jacobsson]

206 House of Lords International Relations and Defence Committee, Second Report of Session 2021–22, [UNCLOS: the law of the sea in the 21st century](#), HL paper 159, para 74

207 International Maritime Organization, [Port State Control](#) (accessed 22 July 2025)

**122.** The UK is a signatory to the Paris Memorandum of Understanding on Port State Control, whose mission “is to eliminate the operation of sub-standard ships through a harmonized system of port State control”.<sup>208</sup> The Paris Memorandum secretariat produces annual white, grey and black lists of flag states, based on the results of port state control inspections.<sup>209</sup> The China Strategic Risks Institute has highlighted this as a potential mechanism for applying pressure to suspicious vessels, and called for the reporting regime to be extended to include:

a joint investigation and reporting mechanism for vessels suspected of subsea cable damage. [...] Investigations could examine patterns of anchoring, trawling, or transiting in protected cable zones for evidence of reckless or malicious behaviour.<sup>210</sup>

**123. RECOMMENDATION**

The Foreign, Commonwealth and Development Office and the Department for Business and Trade should apply diplomatic and economic pressure to press for adequate investigations from flag states and states where vessels suspected of cable damage enter port. The Government should also work with partners, particularly the International Maritime Organization, to make greater use of port state controls as a deterrent—for example by expanding mechanisms to share data on vessels’ behaviour at sea and ensuring these are then thoroughly integrated into port inspections.

---

208 [Paris Memorandum of Understanding on Port State Control](#), including 46th Amendment, 30 May 2025; Paris MoU, [Organisation](#) (accessed 23 July 2025)

209 Paris MoU, [WGB Flag performance list 2024](#), July 2025

210 China Strategic Risks Institute, [Testing the waters: Securing the UK’s subsea cables against grey-zone threats](#), June 2025, p.29

---

# 8 Military and monitoring responses

## Monitoring issues

- 124.** The UK and industry have various monitoring systems, but limitations abound.<sup>211</sup> Coastal radar only covers 22% of the Exclusive Economic Zone (EEZ), supplemented by some aerial monitoring.<sup>212</sup> Systems to track vessel activity, notably the Automatic Identification System (AIS), can be avoided by switching off trackers near sensitive sites.<sup>213</sup> High levels of traffic help malicious actors hide among legitimate shipping.<sup>214</sup>
- 125.** Underwater awareness is even more challenging. The 2022 National Strategy for Maritime Security noted that only 10% of the UK’s global marine area had been mapped to modern standards, “partly caused by challenges with data collection” and co-ordination.<sup>215</sup> The Government told us that “current capabilities cannot fully guarantee that all vessels adhere to UK laws and regulations, especially around sensitive infrastructure like subsea cables”.<sup>216</sup>
- 126.** Underwater sensing is a widely cited option to bring improvements.<sup>217</sup> Alcatel Submarine Networks told us that distributed acoustic sensing (DAS) is one technology which can be integrated into existing cable systems. By monitoring the underwater environment it can detect, locate and report

---

211 [Q15](#) [Captain Niels Markussen]; [Q55](#) [Mick McGovern]; Captain Adrian Pierce RN (Rtd) ([USC0050](#))

212 Home Office, [Planning Aerial Surveillance Service](#), 20 September 2024

213 Windward AI ([USC0021](#))

214 Department for Science, Innovation and Technology ([USC0022](#))

215 HM Government, [National Strategy for Maritime Security](#), CP 724 (2022) Para 16

216 Department for Science, Innovation and Technology ([USC0022](#))

217 E.g. Centre for Peace and Security, Coventry University ([USC0008](#)); Fiber Optic Sensing Association (FOSA) ([USC0014](#)); Professor Timothy Edmunds (Professor of International Security at University of Bristol); Professor Andrew Neal (Professor of International Security at University of Edinburgh) ([USC0018](#)); Department for Science, Innovation and Technology ([USC0022](#)); Alcatel Submarine Networks (ASN) ([USC0030](#)); Chatham House ([USC0045](#)); ICPC, [Submarine cable protection and the environment](#), 2024

threats within two to three kilometres. This might provide up to 14 minutes advance warning.<sup>218</sup> The company highlighted that DAS is already used at Lowestoft and could monitor most of the cables in the UK's EEZ.<sup>219</sup>

- 127.** There are limitations: the sensing signal stops at the first repeater, so monitoring for long cables, notably transatlantic links, would end around 50 kilometres from the shore.<sup>220</sup> We also noted the risk that sensors might accidentally reveal the locations of friendly submarines, not just adversaries. The Government said it would seek to “ensure that emerging technologies like distributed acoustic sensing are deployed safely”.<sup>221</sup>
- 128.** There are other options for making subsea cables a harder target, including deeper burial in vulnerable areas, or tougher armouring.<sup>222</sup> Crosslake Fibre noted however that there are limits to how much physical protection can be added in a cost-effective way.<sup>223</sup>

### A joined-up response

- 129.** The ESCA called for better use of existing rules and data, particularly the AIS regime.<sup>224</sup> Indeximate, a subsea cable data analytics firm, argued that the integration of different sensing and monitoring technologies would deliver major benefits:

By combining DAS with Geographic Information Systems (GIS), Automatic Identification Systems (AIS), and satellite data, we can create a comprehensive defensive network capable of identifying both accidental and intentional threats to subsea infrastructure.<sup>225</sup>

---

218 Alcatel Submarine Networks (ASN) ([USC0030](#)). DAS can also reportedly differentiate between human or natural activity. Centre for Peace and Security, Coventry University ([USC0008](#)). There are various other options, for example SMART cables. See ICPC, [Submarine cable protection and the environment](#), 2024

219 Alcatel Submarine Networks (ASN) ([USC0030](#))

220 Alcatel Submarine Networks (ASN) ([USC0030](#))

221 Department for Science, Innovation and Technology ([USC0022](#))

222 Department for Science, Innovation and Technology ([USC0022](#)), Edmunds and Neal ([USC0018](#))

223 Even well armoured or buried cables can be severed by deliberate damage in shallow waters. See Crosslake Fibre UK Limited ([USC0020](#))

224 European Subsea Cables Association ([USC0026](#))

225 Indeximate Ltd ([USC0023](#)); see also Mr Peter Jamieson (Principal Engineer - Core Fibre and Subsea at Virgin Media O2) ([USC0002](#))

- 130.** Captain Niels Markussen, Director of NATO’s Maritime Centre for Security of Critical Subsea Infrastructure and NATO Shipping Centre, said there were still challenges around analysing data from different sources, such as satellite, radar, and AIS, in an integrated way:

There is a lot of data out there. We just need to systemise the approach.<sup>226</sup>

- 131.** ASN suggested that an extensive deployment of DAS could underpin a more integrated response structure: if DAS threat detection notifications are sent to a national central hub, they could be checked against other identifiers (satellite, radar, and AIS).<sup>227</sup> Vessels deemed suspicious could be contacted by an operator—and if the vessel ignores the warning then the coastguard could investigate.<sup>228</sup>

### Who would pay?

- 132.** The UK has longstanding strengths in ocean monitoring technology for scientific, commercial and military purposes.<sup>229</sup> It is also a centre of expertise in anti-submarine warfare.<sup>230</sup> We noted that a greater focus on subsea cable security may provide opportunities for domestic industries, aligned with the National Security Strategy’s objectives to achieve sovereign capability and benefit UK businesses.<sup>231</sup>
- 133.** There are questions about where the investment should come from. RAND Europe argued that the private sector should take on a “greater role in safeguarding critical subsea infrastructure and adopt a duty of care”. It continued:

The operators of such infrastructure should serve as the first line of defence against hybrid warfare. This means making this infrastructure resilient and secure by design [... which] should include the integration of advanced monitoring techniques.<sup>232</sup>

- 134.** The ESCA did not appear to favour compulsory resilience requirements, suggesting that regulations could “inadvertently undermine broader resilience efforts” by “impeding the timely deployment [ ... ] of subsea cables.”<sup>233</sup> Keith Schofield, former General Manager of the International Cable Protection Committee, suggested the Government could “make a strategic investment on sensors” to address the:

---

226 [Q21](#)

227 On the use of AI tools to analyse maritime data, see Windward AI ([USC0021](#)); RAND Europe ([USC0035](#))

228 Alcatel Submarine Networks (ASN) ([USC0030](#))

229 National Oceanography Centre ([USC0033](#)); University of Plymouth ([USC0013](#))

230 Emma Salisbury, [A New Hybrid Navy](#), Council on Geostrategy, 5 June 2025

231 HM Government, [National Security Strategy](#), 2025

232 RAND Europe ([USC0035](#))

233 ESCA ([USC0026](#))

‘security gap’ between the current protections that already address the peacetime needs of commercial enterprise, compared with the government’s fundamental need to protect its citizens.<sup>234</sup>

**135. RECOMMENDATION**

The Government should support the subsea cable industry in rolling out more extensive cable monitoring technology and should explore incentives to encourage such investment. This could include Government commitments to make better use of existing measures and data—for example more proactive identification and investigation of vessels switching off Automatic Identification Systems. We also encourage industry to engage closely with the Ministry of Defence to ensure underwater monitoring does not unduly compromise defence activity.

## Military activities in peacetime

### Existing action

- 136.** Military operations to protect subsea infrastructure remain difficult: the areas are vast, and assets are scarce. The Royal Navy has been investing in surveillance equipment,<sup>235</sup> and new vessels such as the RFA Proteus.<sup>236</sup> Recent changes to the rules of engagement have enabled warships to get closer to suspect vessels for better observation.<sup>237</sup> The UK has also played a key role in NATO’s “vigilance activity” operations via Baltic Sentry, and the Joint Expeditionary Force’s “response option” Nordic Warden.<sup>238</sup> NATO recently launched its Maritime Centre for Security of Critical Subsea Infrastructure to improve co-ordination.<sup>239</sup>

### Deterrence concepts

- 137.** However, Captain Markussen told us that the military was “not a very good instrument in peacetime” for tackling low-level hybrid threats. He said NATO’s efforts largely consisted of “presence and monitoring”.<sup>240</sup>

---

234 Keith Schofield ([USC0049](#))

235 Policy Exchange, [From space to seabed](#), 2024, pp.48–49

236 Naval technology, [RFA Proteus enters service in the UK’s Royal Fleet Auxiliary](#), 11 October 2023

237 Ministry of Defence, [Defence Secretary oral statement on Russian Maritime Activity and UK Response](#), 22 January 2025

238 Office of the President of the Republic of Finland, [Joint Statement of the Baltic Sea NATO Allies Summit](#), 14 January 2025; Joint Expeditionary Force, [The Joint Expeditionary Force activity NORDIC WARDEN](#), 3 June 2025

239 NATO Allied Maritime Command, [NATO officially launches new Maritime Centre for Security of Critical Subsea Infrastructure](#), 28 May 2025

240 [Qq15–16](#) [Captain Niels Markussen]

We questioned the real-world impact of this as a deterrence concept, particularly for countries like Russia.<sup>241</sup> Professor Kevin Rowlands was circumspect:

How do you protect? You may detect something happening, but how do you protect against that thing happening? Again, we are not necessarily good at that at the moment.<sup>242</sup>

- 138.** Elisabeth Braw of the Atlantic Council similarly suggested more thought needed to go into “what we are going to do”:

Not just when it occurs, but before it occurs, what are we going to signal in our deterrence signalling to other countries? ... The signalling should be, “If we notice suspicious activity, we are going to do X”. What is that X? Nobody has decided what it is going to be.<sup>243</sup>

- 139.** The Minister for Armed Forces argued that monitoring enabled different levels of attribution—for example, technical identification of an offending vessel, intelligence attribution, or publicly calling out bad behaviour. He maintained this did have an impact:

If something happens, and you can pinpoint the vessel only a few nautical miles away from where it has taken place and say, “It was that one”, that provides a much greater deterrence to the master of that vessel, who will realise that consequences could be taken almost immediately if they were to undertake any interference.<sup>244</sup>

The Minister suggested further sanctions could include “seizing the vessel, challenging their licence to operate, affecting their insurance capabilities, prosecuting the people in charge of the vessel at that point or taking further action against the shipping line”.<sup>245</sup> We were uncertain whether these options were limited by the legal complexities outlined in Chapter 7.

- 140.** Some stakeholders called for a more robust approach, possibly involving direction interdiction of a ship, disabling further transit or, in the case of uncrewed vessels, destroying the vessel.<sup>246</sup> This would require close co-operation with enforcement agencies. A brief review of recent case studies (summarised in Table 1) suggests an assertive approach might yield some success, though the Jaguar case also points to the risks of retaliation.

---

241 For examples [Q7](#) (Professor Kevin Rowlands); [Q21](#) (Commodore (Rtd) John Aitken and Captain Niels Markussen); RAND Europe ([USC0035](#)), p.17

242 [Q7](#) [Professor Kevin Rowlands]

243 [Q12](#)

244 [Q65](#) [Luke Pollard]

245 [Q65](#) [Luke Pollard]

246 [Q21](#) [Commodore Aitken], RAND Europe ([USC0035](#)); Captain Adrian Pierce RN (Rtd) ([USC0050](#))

**Table 1. Enforcement actions–selected examples**

Date and location	Suspect activity	Action taken	Consequences
November 2024, Baltic Sea	Yi Peng 3, a Chinese-flagged cargo ship, dragged its anchor for 300km, cutting two subsea cables BCS East-West Interlink (between Sweden and Lithuania) and the C-Lion 1 (between Finland and Germany). <sup>247</sup>	Chinese authorities allowed representatives from Sweden, Germany, Finland and Denmark to board and make observations, but did not allow the Swedish public prosecutor aboard, or for Sweden to carry out a criminal investigation. <sup>248</sup>	Vessel left Danish EEZ two days after the boarding. No crew were arrested or prosecuted. The Swedish authorities were therefore unable to conclude whether cable damage was deliberate or accidental. <sup>249</sup>

247 Statens haverikommission, [SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3](#), 15 April 2025. Translation from the original Swedish via Google Translate.

248 Statens haverikommission, [SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3](#), 15 April 2025. Translation from the original Swedish via Google Translate.

249 Statens haverikommission, [SHK:s observationer ombord på det kinesiska lastfartyget YI PENG 3](#), 15 April 2025. Translation from the original Swedish via Google Translate.

Date and location	Suspect activity	Action taken	Consequences
November 2024, Irish Sea	Yantar, a Russian research ship (allegedly a spy ship <sup>250</sup> ) was detected loitering over UK critical subsea infrastructure. <sup>251</sup>	UK deployed maritime patrol aircraft, two warships and the RFA Proteus to shadow Yantar. A Royal Navy submarine was also authorised to surface near the Yantar. The UK worked jointly with the Irish military, which also sent a vessel to shadow the Yantar. <sup>252</sup>	Yantar ceased loitering and left UK waters south towards. <sup>253</sup>

250 In announcing the measures taken against the Yantar, the UK Defence secretary stated:“Let me be clear, this is a Russian spy ship used for gathering intelligence and mapping the UK’s critical underwater infrastructure.” Ministry of Defence, [Defence Secretary oral statement on Russian Maritime Activity and UK Response](#), 22 January 2025  
 Researchers from the University of Pennsylvania note that the vessel is operated by GUGI, the Russian military’s Main Directorate of Deep-Sea Research. Benjamin Schmitt, Alan Riley, Michał Kurtyka, [Underwater Mayhem: Countering Threats to Energy and Critical Infrastructure Across the NATO Alliance and Beyond](#), May 2025

251 Ministry of Defence, [Defence Secretary oral statement on Russian Maritime Activity and UK Response](#), 22 January 2025

252 Guardian, [Russian spy ship escorted away from area with critical cables in Irish Sea](#),16 November 2024

253 Ministry of Defence, [Defence Secretary oral statement on Russian Maritime Activity and UK Response](#), 22 January 2025

Date and location	Suspect activity	Action taken	Consequences
December 2024, Baltic Sea	Eagle S, a Cook Islands-flagged ship was suspected of deliberately damaging one subsea power cable and three telecommunications cables running between Finland and Estonia. <sup>254</sup>	Finnish authorities boarded the Eagle S and escorted it to port, where the ship was impounded and eight of the 24-member crew detained. Finland’s National Bureau of Investigation launched an inquiry into the incident. <sup>255</sup>	Finland released the ship in March 2025, but has since charged three crew members with “aggravated sabotage and aggravated interference with telecommunications”. <sup>256</sup> The legal basis for Finland’s actions has been debated. <sup>257</sup>

- 
- 254 The Eagle S was allegedly part of the so-called shadow fleet. It had sailed from the Russian port of Ust Luga and was carrying 35,000 tonnes of Russian fuel. Windward AI said that “the Eagle S had numerous transmitting and receiving devices, transforming it into a potential surveillance asset for Russia.” Windward AI, [The Eagle S and the Threat to Underwater Infrastructure](#), 31 December 2024; Guardian, [‘Shadow fleets’ and subaquatic sabotage: are Europe’s subsea internet cables under attack?](#), 5 March 2025
- 255 EuroNews, [Finnish police detain Russian ‘ghost fleet’ ship crew as cable damage probe continues](#), 3 January 2025
- 256 Guardian, [Finland charges tanker crew members with sabotage of subsea cables](#), 11 August 2025; Janes, [Finnish investigation report recommends charges for Eagle S over cable damage](#), 18 June 2025
- 257 Professor Aurel Sari, [Protecting maritime infrastructure from hybrid threats](#), Hybrid CoE Research Report 14, 2025

Date and location	Suspect activity	Action taken	Consequences
May 2025, Baltic Sea	Jaguar, a stateless oil tanker suspected of belonging to Russia’s shadow fleet, was heading to the Russian port of Primorsk. <sup>258</sup> It entered Estonia’s EEZ, and allegedly approached the location of the EstLink subsea power cable. <sup>259</sup>	Estonia sent a helicopter, a patrol plane, and a navy patrol ship to intercept the Jaguar. The ship refused to comply with instructions from Estonian authorities. <sup>260</sup>	Russia sent a SU-35 fighter jet to accompany the vessel, and it briefly entered Estonian air space. In response, Portuguese F-16s (assigned to NATO’s Baltic Air Policing mission) were scrambled from Estonia’s Ämari Air Base. Estonian authorities decided not to board the Jaguar. The Estonian Navy escorted the vessel out of Estonia’s EEZ. <sup>261</sup>

**141. RECOMMENDATION**

The UK’s military deterrence concepts are too timid. They need to place greater emphasis on prevention and punitive consequences that go beyond private or public attribution. Otherwise, aggressors that are content with ‘implausible deniability’ can cause damage with minimal risk to themselves. The Government should work with NATO to ensure that monitoring schemes are designed to enable speedy data sharing with law enforcement authorities—which in turn should support timely investigations, and more direct physical interdiction and prosecution where needed.

258 Lloyd’s List, [Dark fleet politics escalate as Russia scrambles jet to protect ‘nationless’ tanker](#), 15 May 2025

259 ERR News, [Navy escorts suspected ‘shadow fleet’ tanker out of Estonian waters](#), 14 May 2025

260 ERR News, [Navy escorts suspected ‘shadow fleet’ tanker out of Estonian waters](#), 14 May 2025

261 The Estonian authorities allegedly called off the boarding operation mid-way. ERR News, [Experts: Estonia’s failed shadow fleet tanker operation reveals shortcomings](#), 17 May 2025

## Atlantic Bastion

- 142.** The UK's Strategic Defence Review, published in June 2025, set out an 'Atlantic Bastion' concept.<sup>262</sup> The Minister for Armed Forces said the idea was primarily about securing "the North Atlantic from malign Russian naval presence" through traditional anti-warfare capabilities around the Greenland-Iceland-UK Gap, and a network of additional sensors. He explained this would improve defences against ballistic missile strikes but would also help defend cables, because the monitoring systems generate "a greater understanding of what is in your battle space". Key UK assets include P-8 aircraft and Type 26 frigates, alongside NATO contributions.<sup>263</sup>
- 143.** We welcomed this progress, though a review from Andrew Boyd, an industry analyst, suggests the concept still has some limitations:

The Type 26 promises to be an outstanding anti-submarine warfare vessel, but is expensive with only eight vessels planned, allowing one permanently on station from 2030 and two by mid-decade. At current build-rates, none of the promised 12 new AUKUS SSNs [attack submarines] will be operational before 2040 and the need to replace the current Astute Class means no growth in force before the end of that decade ...

Meanwhile, the Royal Air Force has just nine P-8s: excellent state-of-the-art maritime patrol aircraft, but barely a quarter of Cold War strength ... The brutal reality of these numbers constrains British ambition to monitor the vast 'Bastion' area.<sup>264</sup>

- 144.** The availability of assets matters for cables because, in addition to standing tasks and protecting sensitive sites, the military may be called upon to escort repair ships too. When asked about conducting repairs in a security crisis, Alasdair Wilkie of ACMA said that "the answer is probably no [... not] without any military assistance".<sup>265</sup> Mick McGovern of Alcatel Submarine Networks noted that repair ships would be "stationary for two to three days ... and that is quite a big target. A lot of thought has to go into how you

---

262 HM Government, [Strategic Defence Review](#), 2025, p.105. See also Emma Salisbury, [A New Hybrid Navy](#), Council on Geostrategy, 5 June 2025

263 [Q65](#) [Luke Pollard]. Dr Kaushal has previously argued that just covering the GIUK gap would require a major proportion of the UK's available P-8 contingent, and even small gaps in monitoring capabilities "can have a disproportionate impact". See Sidharth Kaushal, [Anti-submarine warfare: A scalable approach](#), European Security & Defence, 24 March 2025.

264 Andrew Boyd, [How Nato can defend the Atlantic](#), Engelsberg ideas, 12 June 2025

265 [Q53](#) [Alasdair Wilkie]

cope”.<sup>266</sup> Matthew Bowden, Director and General Manager at Red Penguin Marine, said the military practices escorting but “the cable ships never practise it, and so operating in that scenario would be quite tricky”.<sup>267</sup>

- 145.** The Minister suggested that gaps may be bridgeable by “a mix of crewed, uncrewed and autonomous vessels” including the Type 92 or Type 93 autonomous vessels.<sup>268</sup> Whilst ambitions to offset limited numbers with technology is welcome, autonomous vessels can be used for offensive purposes too.<sup>269</sup> It remains unclear whether advances will hand defenders decisive advantages.<sup>270</sup> There are further uncertainties about deploying these technologies at sufficient scale, range and duration.<sup>271</sup> Commodore Aitken emphasised there were extensive technical constraints.<sup>272</sup> We were also unsure whether an uncrewed drone escort would provide cable repair ships with sufficient confidence.<sup>273</sup>

**146. CONCLUSION**

In a heightened threat scenario, we are uncertain about the Royal Navy’s ability to protect vulnerable cable regions and escort repair ships without undermining commitments to other NATO tasks. We admire the Minister for Armed Forces’ optimism that the problem can be solved with Atlantic Bastion’s future set of autonomous vessels and monitoring systems. We think there are still quite a few questions to address.

**147. RECOMMENDATION**

The Ministry of Defence should work with international partners to ensure there are viable plans to escort cable ships without degrading wider NATO taskings. This plan could usefully include heightened surveillance of suspicious vessel activity, rules of engagement enabling a low threshold for physical interdiction of civilian and autonomous vessels, and input from industry. The Royal Navy should also practice live escorting exercises with cable repair ships to build confidence about their deployment in a security crisis.

---

266 [Q53](#) [Mick McGovern]

267 [Q8](#) [Matthew Bowden]

268 [Q69](#) [Luke Pollard]

269 [Q8](#) [Professor Kevin Rowlands]; University of Plymouth ([USC0013](#)) Department for Science, Innovation and Technology ([USC0022](#)); APPG for the Ocean ([USC0031](#)); Southampton Marine & Maritime Institute, University of Southampton ([USC0034](#)).

270 Department for Science, Innovation and Technology ([USC0022](#)), RAND Europe ([USC0035](#)), Professor Adam Beaumont (Chairman at aql) ([USC0006](#)); [Q65](#) [Luke Pollard]

271 Policy Exchange, [From space to seabed](#), 2024, p.19; Linden Photonics, [Tethered vs. Untethered ROVs](#), 9 September 2024

272 [Q14](#)

273 [Q68](#) [Luke Pollard]

---

# 9 Governance and planning

## Governance

- 148.** Throughout our inquiry, we heard frequent concerns about governance, co-ordination and oversight of the UK’s subsea cable network.<sup>274</sup> The Government’s written evidence lists 14 relevant departments and agencies engaged in this space, reflecting the variety of maritime activity the Government needs to navigate.<sup>275</sup>
- 149.** For example, the Department for Science, Innovation and Technology leads on telecoms and data infrastructure; the Department for Energy Security and Net Zero covers maritime energy infrastructure; the Ministry of Defence leads on at-sea threats; the Joint Maritime Security Centre “identifies and assesses potential maritime threats” and conducts “routine vessel checks” while the Marine Management Organisation (which has responsibilities around marine planning, some vessel monitoring systems, fisheries and cable repair notifications) sits under the Department for Environment, Food & Rural Affairs.<sup>276</sup>
- 150.** International cable networks are often owned by large consortia, or (increasingly) large tech firms. Information on their data and capacity is often held in confidential contracts.<sup>277</sup> Other actors include operators

---

274 [Q13](#); Windward AI ([USC0021](#)); National Oceanography Centre ([USC0033](#)); RAND Europe ([USC0035](#)); Lieutenant Commander Matthew Brown ([USC0036](#)); Anonymous ([USC0039](#))

275 Department for Science, Innovation and Technology ([USC0022](#)). This includes DSIT, MoD, FCDO, Cabinet Office, Joint Maritime Security Centre (based in the Home Office), HM Coastguard, the Police, National Protective Security Authority, and National Cyber Security Centre. The submission also lists the Department for Environment, Food and Rural Affairs, Department for Energy Security and Net Zero, Department for Transport, Marine Management Organisation, Maritime and Coastguard Agency. (The Crown Estate owns the UK’s territorial seabed and also plays an important role in seabed use planning. The Crown Estate ([USC0052](#))).

276 See Department for Science, Innovation and Technology ([USC0022](#)); [Q57](#) [Sir Chris Bryant]; [Marine Management Organisation](#) (accessed 14 August 2025).

277 For example, the Europe India Gateway is jointly owned by 17 telecommunications carriers. Telegeography, [Submarine Cable Map: Europe India Gateway \(EIG\)](#) (accessed 7 August 2025). See also Jeremy Steventon-Barnes (Chief Technology & Information Officer at EXA Infrastructure) ([USC0029](#))

and maintenance firms, repair agreement groups, and manufacturers.<sup>278</sup> Industry bodies seek to provide join-up,<sup>279</sup> but key information and decision-makers remain quite dispersed.

151. The Government has made some commendable progress to boost co-ordination. A Subsea Infrastructure Response Group (SIRG) works on “coordination of incident planning and response”.<sup>280</sup> The Joint Maritime Security Centre (JMSC), established in 2019, provides an operational security monitoring and co-ordination hub.<sup>281</sup> The Government has launched a project to map data sources on the UK’s subsea infrastructure, and their ownership.<sup>282</sup>
152. DSIT chairs the externally-focused Subsea Communications Cables Industry Group (SCCIG).<sup>283</sup> The Government has joined the European Subsea Cables Association and the International Cable Protection Committee.<sup>284</sup> The UK hosts NATO’s new Maritime Centre for Security of Critical Subsea Infrastructure.<sup>285</sup> The UK engages internationally, recently via the G7 declaration on maritime security.<sup>286</sup>

---

278 Windward AI ([USC0021](#)); Anonymous ([USC0039](#)); European Subsea Cables Association ([USC0026](#))

279 European Subsea Cables Association ([USC0026](#)); [International Cable Protection Committee \(ICPC\)](#), (accessed 14 August 2025)

280 Department for Science, Innovation and Technology ([USC0022](#)). This includes the Cabinet Office, the Ministry of Defence (MoD), Department for Energy Security & Net Zero (DESNZ), the Foreign, Commonwealth & Development Office (FCDO), the Joint Maritime Security Centre, the National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC).

281 The Joint Maritime Security Centre has input from the Department for Transport, the Home Office, and the MoD, supported by the Border Force, the Navy, Counter Terrorism Police, the FCDO, HM Coastguard, HM Revenue and Customs, the National Crime Agency and Marine Scotland. Department for Science, Innovation and Technology ([USC0022](#)); Policy Exchange, [From space to seabed: Protecting the UK’s subsea cables from hostile actors](#), 2024

282 UK Hydrographic Office, [Furthering collaboration on UK subsea infrastructure data](#) (4 August 2025)

283 Department for Science, Innovation and Technology ([USC0022](#)). In 2024 the SCCIG developed the National Emergency Plan for Subsea Fibre Optic Cables—see [Q60](#) [Kevin Adams]

284 Department for Science, Innovation and Technology ([USC0022](#))

285 NATO, [NATO officially launches new Maritime Centre](#), 2024

286 Foreign, Commonwealth and Development Office, [G7 Foreign Ministers’ Declaration on Maritime Security and Prosperity](#), 14 March 2025

## Stakeholder views

- 153.** Many stakeholders were approving of the Government’s progress: Mr Bowden praised the SCCIG as showing “really good strides.”<sup>287</sup> Ms Braw described NATO’s new centre as “a brilliant example of public/private co-operation.”<sup>288</sup> Mr McGovern told us that there had been “a lot of interfacing” with departments to improve awareness of industry’s work.<sup>289</sup>
- 154.** Others highlighted room for improvement. Commodore (Rtd) Aitken thought that “there are a lot of people doing really good work but doing it in isolation without comprehensive oversight”.<sup>290</sup> In written evidence, Lieutenant Commander Matthew Brown said there was “palpable uncertainty” about “jurisdiction and primacy between departments”.<sup>291</sup> The National Oceanography Centre said co-ordination efforts had been largely “ad-hoc” and remained “a work in progress”.<sup>292</sup>
- 155.** One anonymous contributor told us the Government still lacked a “single best view” of the operating environment.<sup>293</sup> Windward AI argued that the JMSC only had “fragmented oversight over privately owned subsea infrastructure”.<sup>294</sup> RAND Europe noted that “some elements of the protection of CUI may be covered by multiple duplicative efforts, while other issues remain unaddressed”.<sup>295</sup>

## A joined-up oversight body

- 156.** Stakeholders generally supported better coordination, though the focus varied across everyday operations, policy, and crisis response. The ESCA called for “a cross-departmental function for ‘Subsea Infrastructure Protection’” providing “a single, coherent point of contact for government interactions with the subsea cable sector” and better join-up with the energy sector.<sup>296</sup> Industry consultant Oluwakemi Adeyanju suggested a single body should be responsible for co-ordinating responses to threats; Commander (Rtd) Adrian Pierce suggested adapting the Joint Maritime Security Centre to have a stronger operational lead from the Ministry of Defence.<sup>297</sup>

---

287 [Q6](#) [Matthew Bowden]

288 [Q12](#) [Elisabeth Braw]

289 [Q47](#) [Mick McGovern]

290 [Q13](#) [Commodore (Rtd) John Aitken]

291 Lieutenant Commander Matthew Brown ([USC0036](#))

292 National Oceanography Centre ([USC0033](#))

293 Anonymous ([USC0039](#))

294 Windward AI ([USC0021](#))

295 RAND Europe ([USC0035](#)), p.20

296 ESCA ([USC0026](#))

297 Oluwakemi Adeyanju ([USC0009](#)); Captain Adrian Pierce RN (Rtd) ([USC0050](#))

- 157.** Others suggested centralising Government oversight of the UK’s subsea cable system data.<sup>298</sup> Lessons might also be learned from the National Energy System Operator, which oversees network health and promotes efficient distribution across the power sector.<sup>299</sup>
- 158.** Vodafone called for a dedicated “Information Sharing and Analysis Centre for subsea cable operators to share real-time data and threat intelligence”.<sup>300</sup> This might emulate the National Cyber Security Centre’s programmes which enable confidential information sharing.<sup>301</sup> This might also address problems outlined by Captain Markussen about firms’ reluctance to disclose vulnerabilities to rivals.<sup>302</sup>
- 159.** There is, however, a risk that a new oversight body might simply add yet another actor into the mix without solving underlying problems—particularly if it did not join up with wider subsea infrastructure around energy installations.<sup>303</sup> The Minister for Data Protection and Telecoms said he was “not convinced” about changing governance structures:

As things stand, I do not think that it is broken, so I am not all that minded to fix it. As a committee, you might come to a different conclusion and persuade us otherwise.<sup>304</sup>

## Crisis responses

- 160.** We had further questions about the adequacy of governance arrangements to handle a fast-moving crisis that exceeds the Government’s current public planning assumptions (explored in Chapter 6). The Minister for Data Protection and Telecoms wrote to us in August outlining response procedures, plans for future exercises, and the role of the Cabinet Office in convening COBR.<sup>305</sup> This appears commendable though, as far as we

---

298 Anonymous ([USC00039](#))

299 Department for Energy Security and Net Zero, [New publicly owned National Energy System Operator to pave the way to a clean energy future](#), 13 September 2024; NESO, [What we do](#) (accessed 14 August 2025)

300 Vodafone Group ([USC0037](#))

301 For example the Cyber Security Information Sharing Partnership. See National Cyber Security Centre, [Building a Security Operations Centre \(SOC\)](#) (accessed 14 August 2025)

302 [Q13](#)

303 The Government’s submission noted that “many of the issues affecting subsea telecoms and energy infrastructure are similar, and having further cross-government coordination of policy work on telecoms and energy infrastructure could potentially help improve identification and understanding of common issues and streamline policy development and messaging”. (Department for Science, Innovation and Technology ([USC0022](#)))

304 [Q57](#) [Sir Chris Bryant]

305 Letter from the Minister for Data Protection and Telecoms to Chair regarding subsea cables, [15 August 2025](#)

could tell, there does not appear to be a well-tested, standing process for identifying critical services' data for rapid rerouting in the event of cascading connectivity failures.<sup>306</sup>

- 161.** If a crisis escalated to near-conflict conditions, clear procedures around repair operations would be critical too. The ESCA's John Wrottesley thought this would require "concerted co-operation" between industry and government:

to make sure that there is the right skilled personnel, availability of kit, joints, cable and so on, and collaboration with the maintenance agreements, to make sure that there is access to those cables that have been damaged so that that can happen. There are a lot of mechanisms for co-operation now, both within industry, and between industry and government, but a lot more could be done to look at this question of national capabilities in a conflict-type situation.<sup>307</sup>

**162. CONCLUSION**

We commend the Government's efforts to improve co-ordination, particularly the establishment of the Subsea Infrastructure Response Group and Subsea Communications Cables Industry Group. We accept that changing governance structures for the sake of it is not helpful. Equally, however, there is evidence that improvements to oversight and co-ordination would benefit day-to-day work and crisis response.

**163. RECOMMENDATION**

The Government should seek to provide a joined-up subsea cables function providing a centralised point of contact for industry and international partners. This body should co-ordinate, not duplicate, cross-government work—bringing together departments and agencies covering subsea infrastructure operations, policy, security, resilience and contingency planning. In the first instance this could involve upgrading the Subsea Infrastructure Response Group into a formal, standing co-ordination and oversight body, reporting into an inter-ministerial group jointly led by the Department for Science, Innovation and Technology and the Ministry of Defence.

---

306 [Q48](#) [Mick McGovern], [Q33](#) [Alex Towers]

307 [Q53](#)

## Spatial planning

- 164.** The seabed around the UK is becoming congested: wind, oil and gas, telecommunications, and marine environmental protection projects are all seeking space.<sup>308</sup> A co-ordinated approach to approving projects is key—otherwise new structures might unintentionally block off critical future cable routes, or funnel cables into a few high-concentration (and hence vulnerable) spaces.
- 165.** The Crown Estate is the independent organisation responsible for managing the seabed around England, Wales and Northern Ireland.<sup>309</sup> It is developing a Marine Delivery Route Map to balance the competing needs of stakeholders.<sup>310</sup> This will:
- assure access to the seabed and coast for subsea telecoms cables in high congestion areas. We are also working to ensure that existing telecoms cables are safeguarded from any future incompatible development.<sup>311</sup>
- 166.** This may involve measures such as reserving key areas for future use by telecommunications cables.<sup>312</sup> Some stakeholders have called for further action.<sup>313</sup> Australia and New Zealand for example have Cable Protection Zones that prohibit certain kinds of anchoring and fishing near cables.<sup>314</sup> These areas are marked on maps and policed through surveillance and patrols. In South Africa such zones extend one mile either side of a cable. APTelecom said Australia’s system is particularly “thorough”, and includes major fines, civil penalties and even prison.<sup>315</sup>

---

308 Crown Estate, [Marine Delivery Routemap](#), 2024

309 The Crown Estate ([USC0052](#)). Crown Estate Scotland owns and manages Crown land in Scotland, including the UK’s territorial seabed off the Scottish coast. See [Crown Estate Scotland](#) (accessed 24 June 2025).

310 Crown Estate, [Marine Delivery Routemap](#), 2024

311 The Crown Estate ([USC0052](#))

312 For discussion on zones versus cable corridors see Communications Security, Reliability and Interoperability Council IV, [Final Report](#), 2014, pp.52–53. See also ICPC, [Government Best Practices For Protecting And Promoting Resilience Of Submarine Telecommunications Cables](#), v 1.2, 2022; Crown Estate, [Submarine cables and offshore renewable energy installations: Proximity Study](#), 2012, p.69

313 APTelecom ([USC0027](#)); Anonymous ([USC0039](#))

314 In Australia, the Australian Communications and Media Authority has the power to designate cable protection zones up to one nautical mile either side of a cable, which can extend into the continental shelf. Australia Communications and Media Authority, [Rules for operating around submarine cables](#), (accessed 14 August 2025); The Communications Security, Reliability and Interoperability Council IV, [Final Report](#), 2014, p.52

315 APTelecom ([USC0027](#)); Anonymous ([USC0039](#))

**167.** Establishing protection zones could be an option for the Government to consider, as it may reduce plausible deniability for malicious actors—or provide greater latitude for imposing tougher sanctions.<sup>316</sup> The Minister for Data Protection and Telecoms said the Government was interested in exploring ideas and was considering the trade-offs.<sup>317</sup>

**168. CONCLUSION**

We support the Crown Estate’s ambitions to improve long-term spatial planning via the Marine Delivery Route Map. We urge those involved to ensure that plans prioritise a diversity of cable routes to avoid creating areas of concentrated targets.

**169. RECOMMENDATION**

The Government should further explore cable protection zones for critical areas of cable concentration, policed by early warning indicators and heightened monitoring and response capabilities. This would require close co-operation with European partners, given the need to manage other maritime activities proportionately.

---

316 Subject to the restrictions on penalising foreign crew outside UK waters, explored in the chapter on legal issues. See also International Law Association, [Submarine Cables and Pipelines under international law \[Third\] Interim Report](#), 2024, para 89

317 [Q71](#) [Sir Chris Bryant]

---

# Conclusions and recommendations

## Overview and trends

1. The UK's strategic reliance on subsea cables will likely continue for the foreseeable future. The cable industry provides a commendable and commercially efficient repair service, which ensures good resilience against moderate damage. We do not believe there is an imminent threat to the UK's national connectivity. (Conclusion, Paragraph 14)

## Threat picture

2. The Government's resilience assessments must take greater account of the worsening security environment over the next 5–10 years. The National Security Strategy and Strategic Defence Review set out serious preparations for future crises. However, the Minister for Data Protection and Telecoms suggested that exploring the risks of a co-ordinated attack on subsea infrastructure was unhelpfully "apocalyptic". We disagree. Focusing on fishing accidents and low-level sabotage is no longer good enough. The UK faces a strategic vulnerability in the event of hostilities. Publicly signalling tougher defensive preparations is vital, and may reduce the likelihood of adversaries mounting a sabotage effort in the first place. (Conclusion, Paragraph 37)
3. We also found sceptical views in some parts of the cable industry about the risks of co-ordinated attacks. We agree that resilience across the sector is generally robust, major disruption is unlikely, and hype is unhelpful. But we caution against adopting 'business as usual' industry views to determine national security risk: individual operators have few financial incentives to prepare for a crisis that may never come. The Government, by contrast, has a duty to prepare competently for low-likelihood, high-risk scenarios. The lessons of 9/11, the financial crash, Covid-19 pandemic and the war in Ukraine are reminders that such events do happen. (Conclusion, Paragraph 38)

4. The Government should update its public and private risk scenarios to cover extensive co-ordinated sabotage to subsea and terrestrial internet infrastructure, including onward connections to Europe. (Recommendation, Paragraph 39)

## System vulnerabilities

5. Many cable landing stations are vulnerable to attack. The Government and operators must take the risk of state-backed sabotage seriously, including against targets in Europe. (Conclusion, Paragraph 47)
6. The National Protective Security Authority (NPSA) and National Cyber Security Centre should require all UK landing stations to be target-hardened to sufficient levels to deter state-backed sabotage. They should require landing station operators to develop within 12 months an emergency ‘good enough’ repair plan to recover from co-ordinated attacks. The NPSA should also conduct a similar exercise with European counterparts for relevant landing stations on the continent. (Recommendation, Paragraph 48)
7. To help mitigate risks around the clustering of high value targets, the Government should encourage subsea cable providers to connect to landing stations, terrestrial routes and data centres outside high-concentration points. (Recommendation, Paragraph 49)
8. The Government’s resilience concept focuses too much on ‘having lots of cables’. This pays insufficient attention to the network’s actual capacity to absorb shocks and does not account for onshore vulnerabilities and long-term trends towards a more brittle system. There is also limited understanding of much damage the system can sustain before data stops rerouting properly, triggering temporary systemic connectivity failure. This does not appear to feature as a serious consideration in the Government’s contingency planning. (Conclusion, Paragraph 62)
9. The Government’s resilience plans should focus in more detail on the level of immediately available capacity in the cable system during a security crisis. The Department for Science, Innovation and Technology should request operators to provide regular updates on the scale and type of data each cable carries, short notice rerouting capacity and their ability to prioritise critical services. It should further develop detailed contingency plans for rerouting data through the Channel Tunnel, including in scenarios where high-concentration terrestrial routes are temporarily disabled. (Recommendation, Paragraph 63)

## Repair vulnerabilities

10. The UK needs more confidence in access to cable repair vessels: the current fleet is ageing, and erstwhile UK businesses have been acquired by foreign entities. (Conclusion, Paragraph 71)
11. The Government should acquire a genuinely sovereign cable repair ship by 2030. This could be leased to industry on favourable terms during peacetime and made available for Government use in a crisis. The Government should set out a timetable for this in response to this Report. (Recommendation, Paragraph 72)
12. The Royal Navy should establish a cadre of reservists and serving personnel to learn cable repair skills on commercial repair vessels. These could be called on in periods of heightened tension. (Recommendation, Paragraph 75)

## Moderate and catastrophic impacts

13. The UK has particular vulnerabilities around outlying islands, the financial sector and military communications cables. These should be a key focus for contingency planning. (Conclusion, Paragraph 81)
14. The impacts of catastrophic disruption from a co-ordinated attack remain speculative, but are almost certainly highly damaging. We estimate they would include payment and supply chain failures, some degraded communications, overstretched emergency responses, and unexpected cascading issues—all at a time of crisis. We are not convinced there are currently adequate sector-by-sector assessments of reliance on subsea cables, or sufficiently detailed plans for handling cascading consequences if data rerouting stops working properly. We are pleased the Government is starting to address this, with a particular focus on the finance sector. (Conclusion, Paragraph 98)
15. The Department for Science, Innovation and Technology should ensure all lead departments have detailed sector-by-sector technical impact studies on areas most likely to be affected and response plans—notably finance, maritime and air traffic, communications, defence and supply chains including food and fuel. We suggest such assessments are handled securely given their value to hostile actors. We note that some cascading impacts may not be immediately obvious—it may therefore be helpful to begin with an underpinning assessment of internet failure modes and how this would affect critical systems. The Cabinet Office resilience teams could usefully help to co-ordinate and audit these assessments. (Recommendation, Paragraph 99)

16. Emergency services should ensure their business continuity plans highlight any areas of critical reliance on foreign internet servers, and account for temporary internet disruption in the event of a security crisis. (Recommendation, Paragraph 100)

## Legal Responses

17. The legal provisions for responding to malicious cable damage are weak. It is encouraging that the Government has identified the forthcoming Defence Readiness Bill as a potential legislative vehicle to implement changes. We would like to emphasise the urgency of making progress internationally too: legal developments can be slow, and the matter is pressing. The UK should use its strong credentials in order to play a leading international role on this topic. (Conclusion, Paragraph 113)
18. The Government's review of legislation must pay particular attention to strong deterrents, such as major fines and criminal liability, that can be applied to private actors suspected of working for or on behalf of foreign states. (Recommendation, Paragraph 114)
19. The Government should explore new options for taking a more robust approach to interdicting suspicious vessels—for example applying piracy provisions to cables that land in the UK or seeking a limited extension of domestic criminal law jurisdiction. It should commission a legal opinion on options and risks, and publish this within six months for consultation with industry and international partners. The Government should, however, remain cautious about the risks of reciprocal action from adversaries and we do not endorse any particular option at this stage. (Recommendation, Paragraph 115)
20. The Foreign, Commonwealth and Development Office and the Department for Business and Trade should apply diplomatic and economic pressure to press for adequate investigations from flag states and states where vessels suspected of cable damage enter port. The Government should also work with partners, particularly the International Maritime Organization, to make greater use of port state controls as a deterrent—for example by expanding mechanisms to share data on vessels' behaviour at sea and ensuring these are then thoroughly integrated into port inspections. (Recommendation, Paragraph 123)

## Military and monitoring responses

- 21.** The Government should support the subsea cable industry in rolling out more extensive cable monitoring technology and should explore incentives to encourage such investment. This could include Government commitments to make better use of existing measures and data—for example more proactive identification and investigation of vessels switching off Automatic Identification Systems. We also encourage industry to engage closely with the Ministry of Defence to ensure underwater monitoring does not unduly compromise defence activity. (Recommendation, Paragraph 135)
- 22.** The UK’s military deterrence concepts are too timid. They need to place greater emphasis on prevention and punitive consequences that go beyond private or public attribution. Otherwise, aggressors that are content with ‘implausible deniability’ can cause damage with minimal risk to themselves. The Government should work with NATO to ensure that monitoring schemes are designed to enable speedy data sharing with law enforcement authorities—which in turn should support timely investigations, and more direct physical interdiction and prosecution where needed. (Recommendation, Paragraph 141)
- 23.** In a heightened threat scenario, we are uncertain about the Royal Navy’s ability to protect vulnerable cable regions and escort repair ships without undermining commitments to other NATO tasks. We admire the Minister for Armed Forces’ optimism that the problem can be solved with Atlantic Bastion’s future set of autonomous vessels and monitoring systems. We think there are still quite a few questions to address. (Conclusion, Paragraph 146)
- 24.** The Ministry of Defence should work with international partners to ensure there are viable plans to escort cable ships without degrading wider NATO taskings. This plan could usefully include heightened surveillance of suspicious vessel activity, rules of engagement enabling a low threshold for physical interdiction of civilian and autonomous vessels, and input from industry. The Royal Navy should also practice live escorting exercises with cable repair ships to build confidence about their deployment in a security crisis. (Recommendation, Paragraph 147)

## Governance and planning

- 25.** We commend the Government’s efforts to improve co-ordination, particularly the establishment of the Subsea Infrastructure Response Group and Subsea Communications Cables Industry Group. We accept that changing governance structures for the sake of it is not helpful. Equally, however, there is evidence that improvements to oversight and co-ordination would benefit day-to-day work and crisis response. (Conclusion, Paragraph 162)
- 26.** The Government should seek to provide a joined-up subsea cables function providing a centralised point of contact for industry and international partners. This body should co-ordinate, not duplicate, cross-government work—bringing together departments and agencies covering subsea infrastructure operations, policy, security, resilience and contingency planning. In the first instance this could involve upgrading the Subsea Infrastructure Response Group into a formal, standing co-ordination and oversight body, reporting into an inter-ministerial group jointly led by the Department for Science, Innovation and Technology and the Ministry of Defence. (Recommendation, Paragraph 163)
- 27.** We support the Crown Estate’s ambitions to improve long-term spatial planning via the Marine Delivery Route Map. We urge those involved to ensure that plans prioritise a diversity of cable routes to avoid creating areas of concentrated targets. (Conclusion, Paragraph 168)
- 28.** The Government should further explore cable protection zones for critical areas of cable concentration, policed by early warning indicators and heightened monitoring and response capabilities. This would require close co-operation with European partners, given the need to manage other maritime activities proportionately. (Recommendation, Paragraph 169)

---

# Formal minutes

**Monday 15 September 2025**

## Members present

Matt Western (Chair)

Tanmanjeet Singh Dhesi

Bill Esterson

Baroness Fall

Lord Hutton of Furness

Baroness Kidron

Edward Morello

Lord Robathan

Lord Sedwill

Lord Tunnicliffe

Baroness Tyler of Enfield

Lord Watts

Sir Gavin Williamson

## Subsea telecommunication cables: resilience and crisis preparedness

Draft Report (*Subsea telecommunication cables: resilience and crisis preparedness*), proposed by the Chair, brought up and read.

*Ordered*, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 169 read and agreed to.

Summary read and agreed to.

*Resolved*, That the Report be the First Report of the Committee.

*Ordered*, That the Chair make the Report to the House of Commons and that the Report be made to the House of Lords.

*Ordered*, That embargoed copies of the Report be made available.

## **Adjournment**

Adjourned till Monday 13 October at 4.00 p.m.

---

# Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the [inquiry publications page](#) of the Committee's website.

## Monday 12 May 2025

**Matthew Bowden**, Director & General Manager, Red Penguin Marine;  
**Elisabeth Braw**, Senior Fellow, Atlantic Council; **Dr Sidharth Kaushal**,  
Senior Research Fellow, Sea Power, Royal United Services Institute (RUSI);  
**Professor Kevin Rowlands**, Visiting Professor, King's College London [Q1-12](#)

## Monday 19 May 2025

**Commodore (Rtd) John Aitken OBE**, Underwater System Services General  
Manager, Thales, former Deputy Director Submarines, Royal Navy; **Captain  
Niels Markussen**, Director, NATO Maritime Centre for Security of Critical  
Undersea Infrastructure and NATO Shipping Centre, NATO [Q13-22](#)

**Dr Marie Jacobsson**, Former Principal Legal Adviser on International Law,  
Swedish Ministry for Foreign Affairs; **Professor Aurel Sari**, Professor of  
Public International Law, University of Exeter, Fellow, Supreme Headquarters  
Allied Powers Europe [Q23-30](#)

## Monday 9 June 2025

**Laura Catterick**, Director, Resilience & Cyber, UK Finance; **Chief Constable  
Gavin Stephens**, Chair, National Police Chiefs' Council; **Alex Towers**,  
Director of Policy and Public Affairs, BT Group; **Dr Fenella Wrigley MBE**,  
Chief Medical Officer and Deputy CEO, London Ambulance Service,  
Ambulance Medical Advisor, NHS England [Q31-46](#)

**Mick McGovern**, General Manager Marine Operations, Alcatel Submarine  
Networks; **Alasdair Wilkie**, Chairman, Atlantic Cable Maintenance & Repair  
Agreement (ACMA); **John Wrottesley**, Executive Director, European Subsea  
Cables Association [Q47-56](#)

## Monday 30 June 2025

**Sir Chris Bryant MP**, Minister of State for Data Protection and Telecoms, Department for Science, Innovation and Technology; **Luke Pollard MP**, Minister for the Armed Forces, Ministry of Defence; **Kevin Adams**, Deputy Director for Telecoms Security and Resilience, Department for Science, Innovation and Technology; **Paul Wyatt**, Director-General for Security Policy, Ministry of Defence

[Q57-72](#)

---

# Published written evidence

The following written evidence was received and can be viewed on the [inquiry publications page](#) of the Committee's website.

USC numbers are generated by the evidence processing system and so may not be complete.

1	APPG for the Ocean	<a href="#">USC0031</a>
2	Adeyanju, Oluwakemi	<a href="#">USC0009</a>
3	APTelecom	<a href="#">USC0027</a>
4	Alcatel Submarine Networks	<a href="#">USC0030</a>
5	Anonymised	<a href="#">USC0039</a>
6	Anonymised	<a href="#">USC0010</a>
7	Archangel Lightworks Ltd	<a href="#">USC0015</a>
8	Beaumont, Professor Adam (Chairman, aql)	<a href="#">USC0006</a>
9	Beck, Roderick (General Manager, Luminous Real Estate And Telecom OÜ)	<a href="#">USC0017</a>
10	Blue Abyss Global	<a href="#">USC0048</a>
11	Brown, Lieutenant Commander Matthew (Mine Warfare and Clearance Diving Officer (RNR), Royal Naval Reserve)	<a href="#">USC0036</a>
12	Centre for Peace and Security, Coventry University	<a href="#">USC0008</a>
13	Chatham House	<a href="#">USC0045</a>
14	Council on Geostrategy	<a href="#">USC0041</a>
15	Crosslake Fibre UK Limited	<a href="#">USC0020</a>
16	Department for Science, Innovation and Technology	<a href="#">USC0022</a>
17	Dr Chapman and Associates Ltd	<a href="#">USC0007</a>
18	Edmunds, Professor Timothy (Professor of International Security, University of Bristol); and Neal, Professor Andrew (Professor of International Security, University of Edinburgh)	<a href="#">USC0018</a>
19	European Subsea Cables Association	<a href="#">USC0026</a>
20	Fiber Optic Sensing Association (FOSA)	<a href="#">USC0014</a>

21	Germond, Professor Basil (Professor of International Security, Lancaster University)	<a href="#">USC0005</a>
22	Guralp Systems Ltd	<a href="#">USC0001</a>
23	Hartmann, Professor Jacques (Professor of International Law and Human Rights, University of Dundee)	<a href="#">USC0040</a>
24	Horizon Bridge	<a href="#">USC0011</a>
25	Indeximate Ltd	<a href="#">USC0023</a>
26	Jisc	<a href="#">USC0019</a>
27	Jamieson, Mr Peter (Principal Engineer - Core Fibre and Subsea, Virgin Media O2)	<a href="#">USC0002</a>
28	Lloyd's Market Association	<a href="#">USC0042</a>
29	Logchem, Dr Yuri Van (Associate Professor in Law of the Sea and International Environmental Law , Norwegian Centre for the Law of the Sea at the UiT-The Arctic University of Norway, Faculty of Law)	<a href="#">USC0024</a>
30	NORBIT LTD	<a href="#">USC0016</a>
31	National Oceanography Centre	<a href="#">USC0033</a>
32	RAND Europe	<a href="#">USC0035</a>
33	RICS	<a href="#">USC0047</a>
34	Pierce RN (Rtd), Captain Adrian	<a href="#">USC0050</a>
35	Sari, Professor Aurel (Professor of Public International Law, University of Exeter)	<a href="#">USC0054</a>
36	Schofield, Mr Keith	<a href="#">USC0049</a>
37	Southampton Marine & Maritime Institute (SMMI), University of Southampton	<a href="#">USC0034</a>
38	Starion UK Ltd	<a href="#">USC0028</a>
39	Steventon-Barnes, Jeremy (Chief Technology & Information Officer, EXA Infrastructure)	<a href="#">USC0055</a>
40	Steventon-Barnes, Jeremy (Chief Technology & Information Officer, EXA Infrastructure)	<a href="#">USC0029</a>
41	Sweeting, Professor Sir Martin (Distinguished Professor of Satellite engineering, Surrey Space Centre, University of Surrey)	<a href="#">USC0051</a>
42	The Crown Estate	<a href="#">USC0052</a>
43	The Hydrographic Society UK & Ireland	<a href="#">USC0038</a>
44	UK Finance	<a href="#">USC0053</a>

45	University of Plymouth	<a href="#"><u>USC0013</u></a>
46	Vodafone Group	<a href="#"><u>USC0037</u></a>
47	Windward AI	<a href="#"><u>USC0021</u></a>