# UK subsea cable vulnerabilities prompt calls for urgent security overhaul



Security vulnerabilities associated with the UK's subsea telecommunication cables have been identified as "abound," according to a recent inquiry by the Joint Committee on the National Security Strategy (JCNSS). These cables, now classified as Critical National Infrastructure (CNI) by the Department for Science, Innovation and Technology (DSIT), underpin much of the nation’s digital connectivity, carrying approximately 99% of UK data traffic through a network of around 60 cables. The committee's report underscores the escalating risks posed by geopolitical tensions and the growing military relevance of UK infrastructure.

The government’s National Risk Register (NRR) 2025 explicitly recognises the threat of a “total loss of transatlantic telecommunications cables,” warning of potentially severe disruptions to internet services, financial systems, supply chains, and essential digital services. While the JCNSS concurs that a complete internet shutdown in the UK remains unlikely under current tensions, it cautions against underestimating a coordinated attack capable of causing significant connectivity failure. The report stresses that current military deterrence is “too timid” and calls for more robust prevention strategies and punitive measures that transcend mere attribution—especially given that adversaries may exploit plausible deniability to inflict damage with limited risk to themselves. It points to particular vulnerabilities around the UK’s outlying islands, military communication cables, and the financial sector, noting that the trend towards high-capacity cables concentrates data into a few high-value targets.

The inquiry challenged an earlier government characterisation of the risk as “apocalyptic,” with the committee pushing back against what it sees as an insufficient focus on more serious and coordinated threats in favour of explanations centred on fishing accidents or low-level sabotage. It advocates for a public stance signalling tougher defensive preparations to potentially deter sabotage efforts by adversaries. The vulnerability extends beyond subsea cables to associated onshore infrastructure such as landing stations and terrestrial links, which the committee finds susceptible to inexpensive but disruptive acts of sabotage.

The JCNSS criticises the industry's reluctance to shoulder the costs of enhanced resilience measures for events deemed low-likelihood but high-impact. The government’s current resilience approach is seen as overly reliant on cable redundancy without adequately assessing the system’s capacity to handle shocks. The report highlights uncertainty over how much damage the cable network can sustain before data rerouting fails, with consequences ranging from moderate disruption to catastrophic outcomes depending on the sector affected.

Reflecting on recent events, such as the suspicious damage to the Estlink 2 power cable between Estonia and Finland—incidentally involving the Russian tanker Eagle S, alleged to be part of Russia’s sanctioned "shadow fleet"—the committee’s findings gain urgency. These incidents reveal a worrying precedent for potential sabotage, reinforcing the need to treat subsea infrastructure as a critical security priority within a complex geopolitical landscape.

The inquiry issues a series of key recommendations to the UK government including updating a legal framework that has remained largely unchanged for 140 years, modernising integrated monitoring and alert systems, and enhancing repair capabilities. Specific proposals call for a UK-flagged sovereign repair ship to speed restoration efforts, reservist training schemes for cable repairs, tougher legal penalties for malicious damage, and closer cooperation with NATO to facilitate rapid information sharing among law enforcement agencies. Additionally, the committee urges more diversified cable routing to avoid creating single points of failure and calls for a dedicated cross-government coordination unit to balance commercial and security interests.

The Ministry of Defence (MoD) has reiterated its commitment to protecting this vital infrastructure and claimed it is investing in “new technologies” to safeguard undersea cables. However, the MoD declined to provide detailed information citing operational sensitivities. The MoD’s position aligns with the increased investment signalled by the recent £2.2 billion rise in defence spending announced in the Spring Budget, although details of how this will translate into improved subsea cable security remain sparse.

On a broader scale, the vulnerabilities of subsea cables also intersect with environmental factors. Research led by the UK's National Oceanography Centre found that natural hazards, including earthquakes and underwater landslides, were responsible for about a quarter of all subsea cable damage recorded between 1965 and 2019. As climate change intensifies such hazards, the risk to these critical networks may increase, adding another layer of complexity to the protection challenge.

Overall, the JCNSS report presents a nuanced picture in which the UK's subsea cable infrastructure is fundamentally resilient but strategically vulnerable in scenarios of heightened hostility or coordinated attacks. It calls for a more assertive and integrated approach to security that combines physical, legal, and diplomatic measures alongside improved monitoring and rapid response capabilities. The government has been given a two-month window to respond to these findings, signalling the importance and urgency attributed to safeguarding the digital lifelines crucial to the UK’s economy and national security.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/), [[4]](https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/206588/how-vulnerable-are-the-uks-undersea-cables-jcnss-publishes-written-evidence/)
* Paragraph 2 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/), [[6]](https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/publications/)
* Paragraph 3 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/), [[2]](https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/209349/uk-too-timid-in-defending-vulnerable-undersea-cables-from-attack-committee-finds/)
* Paragraph 4 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/), [[6]](https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/publications/)
* Paragraph 5 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/), [[4]](https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/206588/how-vulnerable-are-the-uks-undersea-cables-jcnss-publishes-written-evidence/)
* Paragraph 6 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/)
* Paragraph 7 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/), [[5]](https://ukdefencejournal.org.uk/mod-reiterates-commitment-to-protect-to-undersea-cables/)
* Paragraph 8 – [[7]](https://www.marinelink.com/news/noc-natural-disasters-responsible-subsea-525562)
* Paragraph 9 – [[1]](https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/), [[6]](https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/publications/), [[2]](https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/209349/uk-too-timid-in-defending-vulnerable-undersea-cables-from-attack-committee-finds/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.newcivilengineer.com/latest/subsea-cables-security-vulnerabilities-abound-joint-committee-inquiry-reveals-29-09-2025/> - Please view link - unable to able to access data
2. <https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/209349/uk-too-timid-in-defending-vulnerable-undersea-cables-from-attack-committee-finds/> - The Joint Committee on the National Security Strategy has found that the UK government is 'too timid' in defending its vulnerable undersea internet cables from potential attacks. The committee recommends more assertive deterrence measures, including punitive consequences for malicious damage, enhanced monitoring schemes, and improved data sharing with law enforcement. While acknowledging the commendable resilience of the cable industry against moderate damage, the report highlights the need for better preparedness in the event of hostilities, emphasizing the strategic importance of undersea cables to the UK's national security.
3. <https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/204906/how-vulnerable-is-the-uk-to-undersea-cable-attacks/> - The Joint Committee on the National Security Strategy has launched an inquiry to examine the UK's vulnerability to undersea cable attacks. With over 500 cables carrying around 95% of international data, these subsea cables are crucial to the UK's digital infrastructure. The inquiry aims to assess the risks and resilience of these cables, considering potential threats from natural events, accidental damage, and deliberate sabotage, and to evaluate the UK's preparedness for major disruptions to internet infrastructure.
4. <https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/news/206588/how-vulnerable-are-the-uks-undersea-cables-jcnss-publishes-written-evidence/> - The Joint Committee on the National Security Strategy has published written evidence for its inquiry into the vulnerability of the UK's undersea cables. The evidence highlights efforts by states like Russia and China to develop capabilities to attack subsea cables. It also notes that while much internet content is stored in the UK's regional data centres, damage to these cables could disrupt sectors requiring urgent or time-sensitive information, such as finance, defence, news, and government services.
5. <https://ukdefencejournal.org.uk/mod-reiterates-commitment-to-protect-to-undersea-cables/> - The Ministry of Defence has reiterated its commitment to safeguarding critical subsea cables from potential foreign threats. In a response to a parliamentary question, the Ministry stated that subsea cables are critical to UK telecommunications digital infrastructure and that they are committed to maintaining and enhancing the security and resilience of that infrastructure. The Ministry continues to coordinate with partners, including the Department for Science, Innovation and Technology, security partners, the subsea cables industry, and international bodies to assess and understand risks to subsea cables.
6. <https://committees.parliament.uk/committee/111/national-security-strategy-joint-committee/publications/> - The Joint Committee on the National Security Strategy has published various reports and responses, including the 'Subsea telecommunications cables: resilience and crisis preparedness' report. This report examines the security of the UK's subsea telecommunications cables, focusing on preparedness to deal with incidents during periods of heightened international tension or a time-sensitive security crisis. It assesses the adequacy of resilience, contingency plans, and response options, highlighting vulnerabilities and recommending measures to enhance the security and resilience of subsea cables.
7. <https://www.marinelink.com/news/noc-natural-disasters-responsible-subsea-525562> - A study led by the UK's National Oceanography Centre (NOC) has found that natural hazards account for around a quarter of all recorded instances of subsea cable damage between 1965 and 2019. While human activities like fishing and anchoring remain the primary causes of damage, the study warns that climate change is intensifying many natural hazards, increasing risks to these vital networks. The threats from natural hazards range from earthquakes and submarine landslides to powerful underwater currents triggered by river floods.