# Telecom giants warn of rising threats to undersea cables



Major telecommunications companies, including Vodafone, Telefonica, and Orange, have issued urgent warnings regarding a surge in attacks on undersea cables, vital conduits for global internet traffic. These cables are responsible for transmitting approximately 95% of international data, making their security critical for maintaining global internet infrastructure and essential services. The concerns were directed to key international entities, including the European Union, the United Kingdom, and NATO, as disruptions to these cables could lead to significant worldwide ramifications.

The accusations surrounding these incidents have prominently featured Russia, which has been directly implicated by telecom companies, although the nation has strongly denied any wrongdoing. The British Defence Secretary has characterised the sabotage incidents as indicative of Russia’s heightened aggression, calling for increased vigilance and the possibility of retaliatory measures. The situation is exacerbated by the fact that there have been 11 documented cases of cable damage in the Baltic Sea alone since October 2023, with similar occurrences noted in the North Sea. This escalating trend has prompted calls for enhanced international collaboration, including intelligence sharing and joint surveillance initiatives, to safeguard the undersea cable infrastructure.

France has taken proactive steps to bolster the security of its undersea cables in light of past incidents, notably the Nord Stream pipeline sabotage in 2022. President Emmanuel Macron initiated a thorough inspection of French cables and has overseen the implementation of enhanced surveillance measures. In partnership with the French Navy and telecommunications operator Orange Marine, the government has introduced security sensors, underwater drones, and advanced maritime surveillance systems to fortify these critical infrastructures. Nevertheless, experts believe that while the threat of total sabotage exists, the odds remain low, as significant disruption would necessitate the simultaneous severing of multiple major cables. France’s data systems are equipped with redundancies designed to reroute traffic in an emergency, ensuring priority for essential services like hospitals and banks over bandwidth-intensive applications.

The broader global implications of targeted attacks on undersea cables cannot be understated. With more than 500 cables facilitating the bulk of international data, any disruption can lead to cascading effects, jeopardising connectivity and security on a global scale. Experts caution that any hostile action against these infrastructures could be interpreted as a declaration of war, highlighting the urgent need for the international community to prioritise their protection. Initiatives may include utilising satellite monitoring systems and bolstering intelligence-sharing frameworks to secure these sensitive areas.

As geopolitical tensions rise, the need for robust international cooperation to preempt potential threats and safeguard global communications has become increasingly apparent. The future of the interconnected world relies heavily on the resilience and security of these undersea cables, necessitating ongoing commitment from nations to adapt to evolving risks. This includes fostering international partnerships, advancing technological solutions, and implementing comprehensive defence strategies to protect vital communication networks in an era marked by digital interdependence.

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

## References

* <https://www.sustainability-times.com/sustainable-business/policy/total-internet-blackout-incoming-russia-accused-of-global-sabotage-attempt-as-the-us-treats-the-threat-with-maximum-urgency/> - This article reports on the urgent warnings issued by major telecommunications companies, including Vodafone, Telefonica, and Orange, regarding a rise in attacks on undersea cables, emphasizing the critical role these cables play in global internet infrastructure.
* <https://www.telegraph.co.uk/business/2025/04/10/nato-warned-over-internet-blackouts-in-wake-of-subsea-cable/> - The Telegraph discusses NATO's concerns about potential global internet blackouts due to suspected Russian attacks on undersea cables, corroborating claims of escalating threats to these vital infrastructures.
* <https://datacentremagazine.com/networking/the-consequences-of-severed-subsea-communications-cables> - This source outlines the serious global implications of severed undersea cables and the increasing geopolitical tensions that contribute to these vulnerabilities, supporting the need for enhanced protective measures.
* <https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition> - The Center for Strategic and International Studies emphasizes the vulnerability of undersea cables to sabotage and the international implications of their protection, aligning with concerns raised about geopolitical tensions and infrastructure security.
* <https://jeffnewmanlaw.com/u-s-warns-its-telecom-companies-that-their-undersea-cables-are-highly-vulnerable-to-cutting-and-monitoring-and/> - This article highlights U.S. warnings about the susceptibility of undersea cables to foreign tampering, particularly by China, which connects to broader concerns about the security of these cables amid rising geopolitical threats.