Route Sovereignty: The Missing Link in Europe's Digital Sovereignty Agenda

17 OCTOBER 2026

Cliona Hennessy



Photo by Alex Shute on Unsplash

Introduction

To many of us, the internet feels almost ethereal, an invisible current pulled from thin air, carrying information instantaneously from one screen to the next. But the data generated by our digital lives does not simply float around some nebulous cloud in the sky; much of it races beneath our feet through fibre-optic cables laid across the ocean floor. More than 400 of these cables, some no wider than a garden hose, span a combined 1.2 million kilometres across the world's oceans. Yet while Europe has built an extensive regulatory framework governing the data these cables carry, its approach to securing the routes they run along remains far less developed. This article calls this disparity Europe's 'Route Sovereignty' gap: the absence of

an integrated EU approach to controlling and protecting the infrastructure through which European data moves between jurisdictions.

This does not mean the EU lacks cable regulation entirely. The NIS2 Directive (European Parliament & Council of the European Union, 2022a) and the Critical Entities Resilience (CER) Directive (European Parliament & Council of the European Union, 2022b) address some aspects of cable security, such as cybersecurity risk management, physical protection measures and incident reporting. The difficulty, rather, is that cable security remains dispersed across different regulatory frameworks and insufficiently integrated into the EU's wider digital sovereignty strategy. Now, as AI-enabled systems and autonomous technologies threaten to make undersea infrastructure easier to disrupt and responsibility for that disruption harder to trace, this gap is becoming increasingly difficult for Europe to ignore.

Why subsea cables matter

There is no overstating how much Europe depends on subsea cables. They carry over 99% of its intercontinental data traffic (International Telecommunication Union [ITU], 2026), leaving satellites to handle only a small remainder. But vulnerability is not simply a question of volume; it is also a question of location. Cables often cluster along the same transit corridors and share landing points, creating chokepoints where one disruption can affect several connections at once (European Union Agency for Cybersecurity [ENISA], 2023). Nowhere is this concentration more visible than in the Baltic Sea, where shallow, heavily trafficked waters host numerous telecommunications and energy links within a relatively small area. However, a broken cable is not always evidence of an attack. Anchoring and fishing account for nearly 40% of recorded faults, with human activity accounting for 87% of all incidents (ENISA, 2023). Nor does every break produce a crisis: built-in redundancy usually allows traffic to be rerouted when a single link fails. The strategic problem, therefore, is not simply whether a cable breaks, but why it broke and whether that cause can be established with confidence.

Recent incidents in the Baltic have brought this uncertainty into sharper focus. Between November 2023 and January 2025, four separate incidents saw telecommunications cables, power links and pipelines damaged by vessels operating in the region, repeatedly raising the same question: accident or deliberate interference? In a January 2026 report, the EU's Submarine Cable Infrastructures Expert Group acknowledged that distinguishing accidental from intentional damage is "not always easy" (Submarine Cable Infrastructures Expert Group, 2026). Advances in autonomous underwater technology now add another layer to this uncertainty. Rossiter (2025) notes that roughly two-thirds of global seabed infrastructure lies within the three-kilometre diving range already achievable by uncrewed vehicles. Greater technological reach, however, does not automatically make cables more vulnerable: Rossiter also observes that increasing autonomy can benefit

defenders as well as attackers. The technology is therefore changing both how subsea links can be threatened and how they can be protected. Against this evolving landscape, the fundamental question is whether Europe's governance of the infrastructure beneath its digital economy has kept pace with its strategic importance.

The Missing Link in Europe's Digital Sovereignty

Europe's approach to digital sovereignty is extensive. The GDPR governs how personal data is processed and transferred, while recent initiatives have expanded the EU's focus to cloud services, AI, semiconductors and computing capacity. But the physical routes connecting these systems remain far less prominent. Nowhere is this disparity more apparent than in the Commission's 2026 Tech Sovereignty Communication, which commits €120 billion to semiconductors, €200 billion to data centres and €100 billion to cloud and AI leadership (European Commission, 2026b), while making no mention of subsea cable infrastructure as either an investment priority or a resilience concern. Europe's sovereignty ambitions extend deep into the technologies that store and process data, but far less comprehensively to the physical routes carrying it.

This reflects what Carrapico and Farrand (2025) describe as an "autonomy–interdependence gap" between Europe's digital ambitions and its reliance on infrastructure it does not fully control. Rudolph (2026) conceptualises digital sovereignty through three dimensions: data control, legal jurisdiction and vendor nationality. Route Sovereignty adds a crucial physical dimension by asking who protects the infrastructure carrying European data, how easily traffic can be rerouted during a disruption, and how much strategic influence Europe retains over those routes. Put simply, digital control is incomplete without comparable attention to the physical networks carrying the data.

Europe is beginning to address this blind spot. The Commission's 2025 Cable Action Plan (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2025) and Expert Group build on NIS2 and CER, bringing cables onto the digital policy agenda. The challenge is integration. ENISA, the European Fisheries Control Agency and the European Maritime Safety Agency, alongside Commission directorates DG CNECT, DG MOVE and DG MARE, hold partial mandates, while jurisdiction beyond national waters becomes less clear (ENISA, 2023). Private ownership adds another tension. TeleGeography estimates over $14 billion in cable construction by 2027, driven largely by Big Tech (TeleGeography, 2025–2026). This gives private companies considerable influence over where critical routes are built and how they are operated, while governments remain responsible for protecting them and responding when disruption is suspected to be deliberate. Investment may be private, but security, investigation and defence ultimately require public authority. The

Route Sovereignty gap is therefore not an absence of regulation or investment, but incomplete integration between private control of infrastructure, public responsibility for its security and Europe's wider ambitions for digital autonomy.

Ireland: The Route Sovereignty Gap in Practice

Ireland offers a clear empirical test of the Route Sovereignty gap. As an island with no terrestrial alternative to subsea connectivity, its dependence on cables makes the tension between national capability, private ownership and EU resilience particularly visible. Fourteen cables connect Ireland internationally, including four transatlantic links and eight to the UK, but no dedicated telecommunications cable yet provides a direct operational route to mainland Europe (Submarine Cable Infrastructures Expert Group, 2026). For traffic between Ireland and continental Europe, this has meant heavy reliance on routes transiting the UK, which is now outside the EU's legal and security framework.

That dependence is particularly striking given Ireland's role in Europe's digital economy. Its 2019 National Cyber Security Strategy estimated that the country hosted over 30% of EU data (Department of Communications, Climate Action and Environment, 2019), although that figure should be taken with a pinch of salt as it predates the current AI-driven data-centre boom. A serious disruption to UK-linked routes would not necessarily disconnect Ireland, because built-in redundancy allows traffic to be rerouted. However, it would reduce the routes available between a major European data hub and the rest of the Union. Ireland's vulnerability therefore lies not simply in being an island. The deeper problem is that its strategic importance to Europe's digital economy has outpaced the diversity of its connections to mainland Europe.

National protection capacity compounds this problem. The Irish Naval Service operates eight vessels, but limited personnel means only around half are typically active, and none carries sonar capable of detecting activity below the surface (McCabe & Flynn, 2024). Ireland has begun to respond. Its 2026 National Maritime Security Strategy prioritises undersea infrastructure, while amendments to the Defence Act 1954 empower the Naval Service to board and redirect vessels threatening critical infrastructure (Department of Defence, 2026a, 2026b). EU policy is beginning to address the connectivity gap as well. The Cable Projects of European Interest (CPEI) framework proposes a direct Ireland–France–Iberia route to increase route diversity (Submarine Cable Infrastructures Expert Group, 2026). Ireland therefore captures the Route Sovereignty gap particularly clearly. Despite its strategic importance to Europe's digital economy, it remains reliant on concentrated connectivity, constrained national protection and still-developing European coordination.

Accident or Attack? How AI Changes the Threat

Ireland's vulnerability, as the previous section shows, stems from concentrated routes, limited national capacity and coordination that is still catching up. But vulnerability alone does not tell us how great the threat really is. How likely is deliberate interference, and when a cable is damaged, can Europe reliably distinguish an accident from an attack? Most cable damage remains accidental, but that prevalence also creates cover for deliberate interference that can initially resemble a routine maritime incident. Under the UN Convention on the Law of the Sea (UNCLOS), coastal states can rarely act against a foreign vessel in international waters without cooperation from the country where it is registered, with cooperation often slow or withheld (Tammikko, 2025). Uncertain intent and limited enforcement therefore allow seemingly accidental conduct, such as anchor-dragging, to become a deniable means of interference. Redundancy may limit the immediate disruption, but Tammikko (2025) argues that it does little to identify or deter whoever caused it.

It is this difficulty in establishing intent that makes advances in autonomous technology increasingly significant. Rossiter (2025) argues that autonomy currently favours attackers because applications such as mine-laying drones and robotic cable-cutting arms remain simpler and cheaper to deploy than the sensing and repair systems needed to defend against them. Russia's 2022 Maritime Doctrine identifies underwater infrastructure as a potential target of state action (Loik, 2024). The Argus-D, an autonomous underwater vehicle developed by Russia's Rubin Design Bureau, illustrates the emerging capability. With the ability to operate at considerable depth and carry a 300-kilogram payload, it has what Sutton (2026) describes as "clear" offensive potential. But technological capability should not be mistaken for evidence of attack. No AI-enabled manipulation of vessel-tracking signals (AIS) or precision anchor-dragging has yet been documented against a European cable.

AI therefore changes the threat in a more subtle way. There is no evidence that it is already driving attacks on European cables. Instead, autonomous systems could make deniable interference cheaper and easier while making responsibility harder to establish. AI exacerbates an existing problem of attribution rather than creating an entirely new threat. For Route Sovereignty, protecting the route increasingly means being able to establish what happened along it.

AI as Defence, Not Just Threat

AI may complicate the question of who damaged a cable, but it can also provide new ways of finding the answer, strengthening the monitoring and detection capabilities Europe needs to spot suspicious activity before it escalates into full disruption. Rossiter (2025) frames this as a dual-use dynamic: the same autonomous technologies that may lower barriers to

interference can also strengthen surveillance and detection. SEAuAIS, a self-explainable AI model built on vessel-tracking (AIS) data, demonstrates this (Skat-Rørdam et al., 2025). Tested against vessel behaviour surrounding the 2022 Svalbard cable breach, it detected 15 of 16 known instances of suspicious behaviour, showing how AI can sift through volumes of maritime traffic that would be difficult to monitor manually. But its capabilities should not be overstated. Only 21% of its warnings identified genuinely unusual activity, meaning roughly four out of five were false alarms. AI can flag suspicious behaviour, but cannot determine whether it is accidental or deliberately hostile.

Detection is also moving beneath the waterline. The Submarine Cable Infrastructures Expert Group (2026) identifies Optical Fibre Sensing, particularly Distributed Acoustic Sensing and SMART (Science Monitoring And Reliable Telecommunications) cables, as technologies that could turn cables themselves into seabed sensors, detecting vibrations along their length rather than relying solely on vessels or satellites. VIGIMARE's pilot with Cinia already uses changes in light travelling through operational fibre to detect disturbances, with further trials planned for the Baltic, Mediterranean and Irish Sea from 2026. These technologies remain at an early stage, but point towards cables that could eventually help detect threats to themselves.

Better detection, however, is not the same as better protection. NATO's Critical Undersea Infrastructure Coordination Cell and Maritime Centre within Allied Maritime Command (MARCOM) connect naval surveillance with civilian operators, helping turn warnings into coordinated action. AI may therefore help narrow the attribution problem identified above, but it cannot resolve the legal and institutional barriers to acting on that information. The real test for Route Sovereignty is whether Europe can turn a warning into credible attribution, and credible attribution into a coordinated response.

From Data Sovereignty to Route Sovereignty

The limits of AI-based detection point to a wider lesson. Better technology cannot secure Europe's subsea infrastructure if the institutions responsible for acting on that information remain fragmented. The same problem runs through the Route Sovereignty gap more broadly. Control over data, regulation, computing capacity and suppliers cannot guarantee digital resilience if the physical infrastructure connecting those systems remains unevenly protected across institutions and countries. Digital sovereignty cannot stop at the data; it must extend to the routes that make its movement possible.

Europe is increasingly recognising this connection. Since 2024, the Commission's Recommendation on submarine cable infrastructures (European Commission, 2024), the Cable Action Plan (European Commission & High Representative of the Union for Foreign Affairs and Security Policy,

2025), and the Expert Group's reports and Toolbox (Submarine Cable Infrastructures Expert Group, 2025, 2026) have given cable security greater institutional weight, while CPEI funding is beginning to translate policy into investment. Cable governance has therefore moved from relative obscurity to active, if still fragmented, EU attention. The Route Sovereignty gap is not static. It is better understood as incomplete and developing rather than absent.

Closing it requires bringing subsea connectivity into the EU's wider conception of digital sovereignty and directing investment towards the vulnerabilities identified throughout this article, including alternative routes, faster repair capacity and greater geographic diversity. This does not necessarily require another institution. The Expert Group's Toolbox already recommends a single coordinating entity in each Member State for cable security and resilience, closely mirroring the solution proposed for Ireland through MARA. Ireland's coordination problem is therefore not uniquely Irish, but one expression of a wider European challenge. Better monitoring and investigation are equally important. AI may help identify suspicious behaviour, but cannot overcome the legal and institutional barriers to establishing responsibility.

Ireland remains a sharp test of whether these commitments translate into resilience on the ground. Absolute control over every cable is neither realistic nor necessary. What matters is Europe's capacity to understand, protect, diversify and restore the routes on which it depends, and to coordinate responsibility when disruption occurs. Route Sovereignty therefore extends digital sovereignty beyond control of the data to resilience of the physical networks that carry it.

Conclusion

Europe's digital sovereignty ultimately rests on something far more physical than the term suggests. The cables beneath its surrounding seas carry the data on which its digital economy depends, but their security has not developed with the same coherence as the rules governing that data. The Route Sovereignty gap is therefore real, although it is a gap of fragmentation rather than neglect. Ireland makes the consequences particularly visible, with a major EU data hub still heavily dependent on routes through a non-EU state while national protection capabilities and European coordination continue to develop. AI adds another layer to this challenge, potentially making interference harder to trace while also offering new tools to detect it. Technology alone, however, cannot substitute for resilient routes, clear responsibility and coordinated action.

Europe does not need to control every cable beneath the sea to claim digital sovereignty. What it does need is the capacity to understand where its critical routes run, protect and diversify them, establish responsibility when disruption occurs and restore connectivity quickly. The EU has

begun moving in that direction, but Route Sovereignty remains incomplete. Europe has spent years strengthening sovereignty over its data. The next challenge lies beneath it.

References

Bandura, R. (2025). *The strategic future of subsea cables: Ireland case study*. Center for Strategic and International Studies.

Bhalla, A. (2026). *Europe must address the digital sovereignty triad*. Atlantic Council.

Brown, E. (2025). *The Baltic Sea at a boil: Connecting the shadow fleet and episodes of subsea infrastructure sabotage*. Carnegie Endowment for International Peace.

Bueger, C. (2025). *The hidden maritime frontier of artificial intelligence*.

Carrapico, H., & Farrand, B. (2025). EU data sovereignty: An autonomy–interdependence governance gap? *Politics and Governance*, *13*, Article 10331.

Davenport, T. (2015). *Submarine cables, cybersecurity and international law: An intersectional analysis*.

Department of Communications, Climate Action and Environment. (2019). *National cyber security strategy 2019–2024*. Government of Ireland.

Department of Defence. (2026a, February). *National maritime security strategy 2026–2030*. Government of Ireland.

Department of Defence. (2026b, March). *New legal powers for Naval Service* [Press release]. Government of Ireland.

Edwards, C., & Seidenstein, N. (2025). *The scale of Russian sabotage operations against Europe's critical infrastructure*. International Institute for Strategic Studies.

European Centre for Development Policy Management. (2026). *Troubled waters: Europe's subsea telecommunications network* (Briefing Note No. 208).

European Commission. (2024, February 26). *Commission Recommendation on secure and resilient submarine cable infrastructures*.

European Commission. (2026a, June). *CEF-Digital second call for proposals to increase Europe's submarine cable repair capacities*.

European Commission. (2026b, June 3). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European tech sovereignty, accompanied by an EU open source strategy*.

European Commission. (2026c). Guarding Europe's hidden lifelines: How AI could protect subsea infrastructure. *Horizon Magazine*.

European Commission. (2026d, February 5). *Submarine cable repair capacities*.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2025, February 21). *EU action plan on cable security* [Joint communication].

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2026, March). *Joint communication to strengthen the security and resilience of submarine cables*.

European Parliament & Council of the European Union. (2022a). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, *L 333*.

European Parliament & Council of the European Union. (2022b). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER Directive). *Official Journal of the European Union*, *L 333*.

European Union Agency for Cybersecurity. (2023). *Undersea cables: What is at stake?*

Finnish Security and Intelligence Service. (2026). *National security overview 2026*.

Institute of International and European Affairs & Vodafone. (2026). *Secure connections: Ireland's digital infrastructure and the resilience of European connectivity*.

International Telecommunication Union. (2026). *International Advisory Body on Submarine Cable Resilience: Report of the working groups 2026*.

Jones, B. D. (2026, February 13). Seabed zero: Baltic sabotage and the global risks to undersea infrastructure. *Bulletin of the Atomic Scientists*.

Loik, R. (2024). Undersea hybrid threats in strategic competition. *Journal on Baltic Security*.

McCabe, R., & Flynn, B. (2024). Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure. *European Security*.

Mok, C. (2026). Toward undersea cable resilience: The case for global collaboration. *Texas National Security Review*.

Rossiter, A. (2025). Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs). *Marine Policy*, *171*, Article 106434.

Skat-Rørdam, H. V., Kjærsgaard, R. D., Hovad, E., & Clemmensen, L. K. H. (2025). SEAuAIS: A self-explainable autoencoder with AIS-based maritime anomaly detection. *Ocean Engineering*, *341*, Article 122656.

Submarine Cable Infrastructures Expert Group. (2025). *Security and resilience of EU submarine cable infrastructures*. European Commission.

Submarine Cable Infrastructures Expert Group. (2026, January). *Submarine cable security toolbox and Cable Projects of European Interest*. European Commission.

Sutton, H. I. (2026, January 2). *Russian XLUUV concept: Argus-D*. Covert Shores.

Tammikko, T. (2025). *The EU and NATO in pursuit of better deterrence: Baltic Sea sabotage prompts rethink of current practices* (Briefing Paper 02/2025). Finnish Institute of International Affairs.

TeleGeography. (2025–2026). *Global bandwidth research service: State of the network*.

UK Parliament, Joint Committee on the National Security Strategy. (2025a). *Subsea telecommunications cables: Resilience and crisis preparedness*.

UK Parliament, Joint Committee on the National Security Strategy. (2025b, December 18). *Subsea telecommunications cables: Resilience and crisis preparedness: Government response*.

Wall, C., & Morcos, P. (2021). *Invisible and vital: Undersea cables and transatlantic security*. Center for Strategic and International Studies.

Windward. (2026). *Q2 2026 undersea cables risk report*.