JULY 2025

The Strategic Future of Subsea Cables

Ireland Case Study

By Romina Bandura and Thomas Bryja

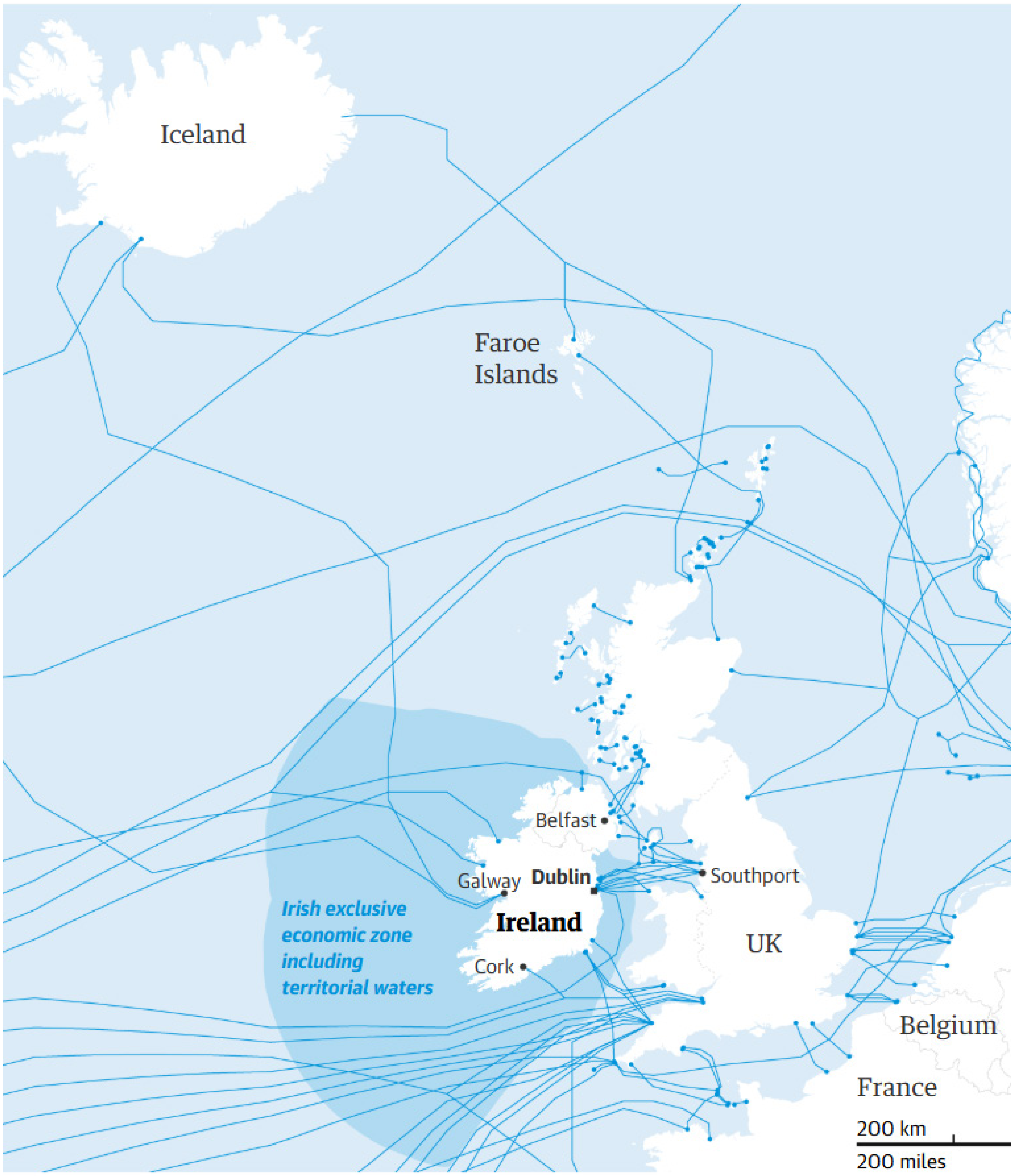
Introduction

Ireland's unique strategic position—linking transnational telecommunications cables between the United States, the United Kingdom, and continental Europe—makes it a key player in safeguarding subsea fiber-optic cables. In 1858, the first **transatlantic** telegraph cable was laid from Kerry, Ireland, to Newfoundland, Canada, marking the beginning of a revolution in global communication. Today, approximately **three-quarters** of subsea cables in the Northern Hemisphere pass near or through Irish waters, making it a critical nexus for international connectivity (see Figure 1). Worldwide, these cables are essential not only for everyday internet and communication but also for financial transactions, processing around **$10 trillion** daily. As technology develops, submarine fiber-optic cables will only prove more critical as the demand for services reliant on them grows.

Despite concerns about energy consumption and grid capacity, Ireland—particularly Dublin—is already a **global hub** for data centers, attracting major tech companies such as Google, Meta, and Amazon with its pro-business environment, skilled workforce, and access to the EU single market. The need for **data centers** will continue to accelerate in the wake of the artificial intelligence (AI) revolution, as training large language models takes enormous, distributed storage to compute; if those networks are globally oriented, they will require additional subsea capacity to connect them. Older cables will need to be replaced as well, as cable lifespans range from **17 to 25** years. In addition, Ireland hosts the European headquarters of major U.S. multinational corporations (MNCs), which rely on its energy and subsea cable infrastructure, underscoring the need to protect and ensure redundancy for these systems.

At the same time, geopolitical tensions have risen worldwide, and Ireland's long historical attachment to neutrality has been prodded in recent years. A May 2021 ransomware attack on Ireland's health services and Russian military exercises off the Irish coast in 2022 prompted Dublin to recognize in

Figure 1: Subsea Cable Network in and near Ireland



Source: "Calls for Ireland to boost defence of subsea internet cables," January 25, 2025, *The Guardian*, https://www.theguardian.com/world/2025/jan/25/could-ireland-longheld-neutrality-make-it-vulnerable-to-infrastructure-attacks.

its **Report of the Commission on the Defence Forces** that "in an era of intensified great power competition, Ireland can expect . . . a growing risk that Ireland's land, air, maritime, and cyber domains become vectors of attacks on or threatening moves against Ireland's neighbors and European partners." Beyond subsea fiber-optic cables, attacks on strategic maritime infrastructure, such as the Nord Stream 2 gas pipelines in 2022, have highlighted the increasing threats to undersea networks.

As the world becomes more interconnected, the accidental or intentional disruption of maritime infrastructure (including subsea cables, gas pipelines, and offshore wind farms) can affect the global economy. A widespread subsea cable failure could potentially **debilitate** certain countries or even entire swaths of the continent in the cyber domain. The security of subsea infrastructure off Ireland's coasts is therefore an essential component of the world economy and international security. The following country case study provides an overview of Ireland's subsea cable infrastructure, highlighting key risks and presenting strategic recommendations for how to expand and protect this critical infrastructure.

Overview of Subsea Cable Infrastructure in Ireland

Ireland's global positioning is of great importance to the country as it seeks to maintain strong international relationships and economic influence. Since the **1990s**, Ireland has pursued a strategic **approach** to attracting foreign direct investment (FDI) through a **combination** of tax incentives, EU market access, and a highly educated workforce. As a result, Ireland is now home to nearly 970 U.S. multinational companies that together **directly employ** approximately 211,000 people, including in sectors such as technology, pharmaceuticals, and finance.

MNCs operating in Ireland are more concerned with emerging issues—such as AI management, energy security, and potential changes in EU regulations—than the risks associated with subsea cable disruptions. However, any widespread disruption to these cables would have significant economic and security repercussions for the country and the safety and reliability of companies' operations.

Despite the significant number of subsea cables crossing Irish territorial waters, Ireland is only connected to this network via **14 cables**: four to North America, one to Iceland, and nine to the United Kingdom. No cables are currently connected to the European mainland, although several are under construction. The first, the **Far North Fiber** cable, backed by five Nordic countries and EU funds, aims to link Ireland, Alaska, Japan, and Norway by 2026. By 2027, the **Celtic Interconnector** will connect Ireland with France. Another subsea cable, the **Polar Connect**, will take a more direct route through the North Pole to connect Europe with North America and East Asia. And the **Pisces** subsea cable will establish links between Ireland, France, Portugal, and Spain.

Not only are there at least four planned subsea cable projects directly landing in Ireland, there are several broader international initiatives in which Ireland is envisioned as a connection point as part of a larger transcontinental network or energy infrastructure. Major investors include tech giants, known as "hyperscalers," such as Amazon, Google, and Meta, which have together funded the **Havfrue** cable that links Ireland, Scandinavia, and the United States. Amazon is planning a **cable** between Cork and the U.S. East Coast, while Microsoft is developing three new **cables** connecting Ireland to Wales (SOBR1, SOBR2, and Tuskar). In addition, **Meta**—which has spent **billions** of dollars on subsea cable projects in Europe—plans to integrate Ireland into its transatlantic cable system, which includes the Amitié connection between the United States, the United Kingdom, and France.

Other key players include Exa Infrastructure, which invested in the **Havfrue** line and **purchased** the Hibernia Atlantic lines for nearly $2 billion. Exa's subsidiary, Aqua Comms, controls several major subsea cable lines, including **CeltixConnect-1**, **AEC-1**, **AEC-2**, and part of **AEC-3**. Tiger Infrastructure Partners financed the **Celtic Interconnector** subsea cable that will link Ireland to France, while **EirGrid**, Ireland's state-owned electric power transmission operator, owns and operates the East-West interconnector linking Ireland's energy grid to that of the United Kingdom.

These planned subsea cable projects aim to enhance connectivity in the Irish Sea and beyond, taking advantage of Ireland's recent boom in data centers. With **82** data centers and 14 more under construction—aided by Amazon's investment of almost **$11.9 billion** through Amazon Web Services since 2012—Ireland has become an **attractive** site to invest in subsea cables and digital infrastructure.

To support this digital expansion, in March 2024, the Irish government issued "**Powering Prosperity: Ireland's Offshore Wind Industrial Strategy**," which promotes offshore renewable energy investments, aiming for 37 gigawatts of offshore wind capacity by 2050 through a €100-billion plan focused on infrastructure, supply chains, and innovation. These investments would not only secure additional sources of energy but also ensure the functioning of Ireland's data centers and subsea cables, which will be vital for meeting the increasing demand for connectivity and energy in the coming years. However, while subsea cable projects generally face little public resistance, offshore wind initiatives have encountered legal challenges from fishermen concerned about their impact on traditional livelihoods. While Ireland has historically focused on fishing as the primary use of its maritime space, it is now recognizing the broader strategic importance of its marine territory, particularly for energy security and telecommunications.

Building, Repairing, and Protecting Subsea Cable Infrastructure

Compared to energy infrastructure in Ireland, which tends to be centrally planned, the country's telecom cable development is developer-led. Subsea cables are primarily built, operated, maintained, and repaired by a small group of private sector companies such as HMN Tech, FiberHome, SubCom, Alcatel Submarine Networks (ASN), and NEC. Only two are involved in the subsea cables around Ireland. First, France's ASN is responsible for the France-U.S.-UK Amitié, **Apollo**, and **FLAG Atlantic-1** connections, as well as the CeltixConnect-1 and CeltixConnect-2 subsea cables between Ireland and the United Kingdom. U.S. company SubCom oversees the maintenance and infrastructure of the **EXA Express**, **IRIS**, Havfrue, **Atlantic Crossing-1**, and **Grace Hopper** transatlantic cables, as well as the **ESAT-2** line between Ireland and the United Kingdom and the **FLAG Europe-Asia** connection. The smaller UK company Vodafone co-owns the Apollo and Amitié cables and owns the **Lanis-3**, **Lanis-2**, **Lanis-1**, and **Solas** lines in the Irish Sea, as well as the planned **Beaufort** connection between Ireland, the United Kingdom, and France.

With regard to the government's role, Ireland has no **single** agency tasked with overseeing subsea cable governance; instead, responsibility is fragmented across multiple departments and state agencies involved in infrastructure oversight and security:

- The **Department of Transport** oversees the **Irish Coast Guard**, which manages maritime casualty and rescue operations in Ireland's exclusive economic zone (EEZ), and the Irish Maritime Administration, which ensures maritime safety and port security.

- Under the **Department of Defence**, the Irish Naval Service (**INS**) enhances maritime defense. Irish forces conduct routine surveillance of foreign vessels with Naval Service assets and Air Corps maritime patrol craft. Foreign vessels are monitored remotely around the clock from the Naval Operations Command Center. A newly established **Maritime Security Unit** is tasked with developing the National Maritime Security Strategy and coordinating future efforts across national and international stakeholders. However, Ireland currently has only one official acting as minister for both defense and for foreign affairs and trade, two heavyweight agencies; it is possible that each might not be receiving their full due attention.
- Through its National Cyber Security Center, the **Department of Justice, Home Affairs and Migration** oversees cybersecurity defense and resilience across government and society.
- The **Department of Climate, Energy and the Environment** is in charge of information technology connectivity and communications. Under its aegis, the independent **Maritime Area Regulatory Authority** (MARA) serves as the principal permitting authority for Ireland's maritime and subsea infrastructure, including for subsea telecom cables, offshore wind farms, and energy interconnectors. Established in 2023, it grants Maritime Area Consents (MACs) for the right to occupy the maritime area, dispenses Marine Usage Licences for certain uses of the maritime area to developers, and conducts regulatory and environmental evaluations. It further enforces compliance with licenses and consents, handles investigations and prosecutions, and promotes cooperation among maritime regulators.

This fragmented and uncoordinated governance structure, combined with a general under-prioritization of Ireland's maritime defense capabilities, has led to concerns about the country's preparedness to handle maritime security threats. Ireland's first legislative framework protecting subsea infrastructure dates to 1884, when the country was part of the United Kingdom, under the **Convention for the Protection of Submarine Telegraph Cables**. This was succeeded by the **Submarine Telegraph Act** of 1885, which recognized threats to subsea cables, such as sabotage and damage from fishing activities. Under an independent Ireland, the **Foreshore Act** of 1933 further established that the sea area is state property, requiring licenses for subsea construction or laying cables. The **Maritime Security Act** of 2004 grants the Irish Navy the authority to intervene against unlawful actions at sea, including damage to subsea cables. More recently, the **Maritime Area Planning Act** of 2021 created MARA to oversee permissions for subsea infrastructure projects, among other functions, and the **Maritime Jurisdiction Act** of 2021 defined Ireland's maritime jurisdiction in accordance with the 1982 **UN Convention on the Law of the Sea** (UNCLOS).

BUILDING NEW CABLES

To build and repair a cable, consents and permits must first be **granted** by MARA, which is responsible for "assessing applications for [MACs] which will be required before developers of offshore wind and other projects in the maritime area can make a planning application." Unlike many other countries, Ireland does not require a separate operator's license or special state permission for such applications. After receipt of a MAC, a developer obtains planning permission, covering not just the cable's maritime components but also its landfall and terrestrial ones, from the national planning board. The process includes environmental impact assessments that can take 12-36 months, involving public consultation, appeals, and possibly judicial reviews, all before a company is approved to build a new cable. Under the

Maritime Area Planning Act, MARA is also responsible for enforcing environmental conditions that may be attached to cable-related projects in the nearshore area.

MARA aims to act as a **one-stop shop** by issuing authorizations at the installation stage that also cover future maintenance and repairs, so operators do not need to request separate permits for each intervention. In practice, however, MARA has no ability as a civilian agency to monitor or defend existing subsea cables, nor does it have its own vessels, so it depends on interagency coordination for incident investigations, response, and enforcement.

The multiple consents and long timelines resulting from this regulatory complexity prove a source of frustration for private sector entities that prefer clear, short timelines if they are to invest the upwards of $200-400 million in capital **required** for building new cables.

REPAIRING EXISTING CABLES

Damage to a subsea cable can occur from a man-made accident, a natural disaster, or intentional damage. As with subsea cables worldwide, the primary threat to those around Ireland is accidental and natural damage, mainly caused by fishing vessels and weather-related events. However, given the current geopolitical moment, a more ominous threat looms in the minds of policymakers: intentional sabotage by state or nonstate actors.

Whether accidental or not, several cable breakages in the **Baltic Sea** over the past few years have proved the vulnerability of these systems and reinforced these fears. The confusion and concern surrounding these cuts reminded Europe that cables could be disrupted intentionally. Certain nation-state actors have openly declared their willingness to do so, with Deputy Chairman of the Russian National Security Council Dmitry Medvedev, for example, **endorsing** the legitimacy of attacking subsea cables.

In February 2020, Irish security services reportedly **accused** Moscow of planting agents in the country in order to map submarine cables and landing stations. In 2021, a cyberattack targeted Irish health services, highlighting the rising threats in the digital domain. The same year, the Russian vessel *Yantar* was spotted deploying a deep-sea mini-submarine off the Irish coast. The vessel, which had been involved in **previous** cable-probing incidents, was **following** the proposed Celtic-Norse cable and the AEC-1 cable, which links Europe to the United States. More recently, in **November 2024**, the *Yantar* was escorted from the Irish Sea after it was caught patrolling above subsea cables and operating three drones. And in **March 2025**, a cargo ship linked to the Russian **shadow fleet** was seen dropping an anchor close to an undersea cable in Irish waters.

If a subsea cable is damaged, the private sector network operator (or the owner) is alerted, and (depending on the jurisdiction and regulatory framework) typically has a legal duty to notify the appropriate national authorities, such as telecom regulators, coast guards, or cybersecurity agencies. In the European Union, **under Article 23 of the Network and Information Systems Directive 2** (NIS2), "operators of essential services"—such as telecommunications companies—must notify the national Computer Security Incident Response Team (CSIRT) or other competent authority within 24 hours of becoming aware of any severe disruptions. This notification must include an initial assessment of whether the disruption was malicious or unintentional and whether there are potential cross-border implications. Within 72 hours, a more detailed assessment of the severity and indicators of compromise must be submitted. Ultimately, it is incumbent upon each EU member state to make this into national law and properly designate authorities for receiving notification. In Ireland, the National Cyber Security Centre (NCSC) **serves as the CSIRT** and oversees compliance with the NIS regulations.

The operator or owner of the cable then **commissions** a repair ship to locate and retrieve the damaged section, splice in a replacement, and return the cable to the seabed, often burying it if the segment lies in shallower waters to protect against future damage. Globally, there are a **limited** number of highly specialized repair ships for such incidents, so awaiting the arrival of a repair ship, plus the actual repair time, can leave a cable offline for weeks (assuming no permitting hiccups).

If an attack occurs **within the first 12 nautical miles** off the coast, Ireland exercises full sovereignty and can take unilateral action as if the incident occurred on land. All the relevant authorities—including the Irish Police, the Irish Coast Guard, the NCSC, and the Commission for Communications Regulation—have full investigative and enforcement powers.

Beyond 12 nautical miles but within 200 nautical miles is Ireland's EEZ, the maritime space within which it has enforcement jurisdiction over economic activities. In practice, the responsibility for **securing** those waters often falls on the **INS**; however, issues with recruitment and retention have limited the capabilities of both its sea and air fleets to effectively undertake the broader maritime security responsibilities of the state.

Under Irish national law and UNCLOS, vessels can face fines and legal liability if they accidentally break a subsea cable, particularly if they are found to be **negligent** or operating in violation of regulations (e.g., trawling in restricted areas). Assessing this often relies on the **Automatic Identification System** (AIS), which provides identification and positioning **information** to ships and land stations. The data can be used to track activity in the area and determine if any ships were involved in the damage. However, if a ship cuts the cable intentionally, it may choose to disable its AIS so it cannot be tracked, further complicating the monitoring process. So far, however, no intentional cable cuts or damages have taken place in Irish waters.

PROTECTING SUBSEA CABLE NETWORKS

Industry actors and the Irish government remain misaligned about who should bear the responsibility and cost of monitoring and protecting this type of infrastructure. As subsea cables are privately owned, in principle, it is the responsibility of the companies to protect the infrastructure. However, any disruptions to these cables would have far-reaching consequences for Irish society (in terms of communications and the economy) since government and business operations rely on them to function. This **infrastructure** represents a crucial component of global financial systems, and intentional damage may pose significant national security risks. Therefore, safeguarding subsea cable networks is not only a private concern but also a national and international one, highlighting the critical need for active government involvement on this front.

Although the sheer scale and complexity of the subsea network make safeguarding it challenging for both companies and government authorities, Ireland is in a particularly vulnerable position given its limited protective capacity, a result of its longstanding position of neutrality and reliance on the United Kingdom to oversee this infrastructure. The country currently invests approximately **0.2 percent** of its GDP in defense, significantly lower than other formerly neutral countries such as Sweden, which invests around 1.5 percent. Ireland's maritime power is under-resourced and understaffed to an unprecedented degree. Drastic **labor shortages**—with crew numbers having dropped by **25 percent** since 1998—resulted in only half of INS ships being active at sea as of 2021, and Ireland subsequently reduced its active fleet to **just two ships in 2023**. Such a lack of credible subsea security capability puts Ireland, the European Union, NATO, and the world's communication and economic security at risk. Ireland's resources are also drastically overstretched, tasked with safeguarding an EEZ encompassing an area of approximately 450,000 square kilometers (170,000 square miles), or roughly **ten times** the size of **Ireland's landmass**.

Perhaps due in part to Russia's war of aggression against Ukraine, the Irish government has recognized and elevated subsea cables as a national defense priority. While the **National Cyber Security Strategy** (2019-2024) does not discuss subsea cables, the 2022 **National Cyber Risk Assessment** prepared by the Department of Climate, Energy and the Environment does have a section dedicated to their importance. Moreover, the 2023 **National Risk Assessment** coordinated by Ireland's Department of Defence includes damage to undersea infrastructure as one of the key risks facing Ireland. Importantly, the 2024 **Defence Policy Review** prompted the Irish government to begin drafting a national maritime security strategy, with a final version **expected** to be published by the end of 2025.

Ireland collaborates with international partners to bolster subsea cable security. As a member of the EU **Permanent Structured Cooperation on Defence and Security**, it participates in European defense cooperation initiatives aimed at strengthening security. It is also part of the **Connecting Europe Facility** Digital Work Program, which signed 21 grant agreements in **December 2024** to enhance submarine cable infrastructure across the European Union.

Although not a NATO member, Ireland participates in the alliance's **Partnership for Peace** program, allowing for greater cooperation on maritime security, intelligence sharing, and defense against cyber and hybrid threats. It is also a member of the **International Telecommunication Union**, a UN agency overseeing global telecommunications and digital connectivity efforts.

In October 2024, Ireland hosted **the Inaugural Symposium on Subsea Cable Security and Resilience** (known as the Valentia Conference), where Irish and international experts across industry, academia, and government convened to address critical issues related to subsea cables. Two months later, the Irish and Icelandic Departments of Defence conducted **a joint workshop** on the security, resilience, and crisis management of critical undersea infrastructure, with Secretary General Jacqui McCrum of the Irish Department of Defence stating:

> Ireland and Iceland's waters are home to critical infrastructure that is of both national and global significance. But we cannot rely on our geographic isolation for our security, nor isolate ourselves from world events. We have a responsibility, through our defence policy, to invest in the defence of the state, to protect our citizens, our values and our sovereign interests and to continue to contribute to international peace and security.

Most recently, Irish Defence Forces purchased an **$80 million** sonar system to protect subsea cables and gas pipelines extending 370 km from its western coast. The system is expected to be completed in 2027 and will monitor the Irish EEZ for ships or submarines seeking to interfere with critical undersea infrastructure.

In sum, the protection and expansion of subsea cable infrastructure around Ireland faces several intertwined challenges:

- **Bureaucratic inefficiencies** proliferate since responsibilities are spread across various government agencies, complicating the expansion and maintenance of subsea networks.
- **A lack of dialogue** between government agencies and private companies exacerbates these inefficiencies, making it more difficult for stakeholders to exchange perspectives on their priorities and perceived threats.
- **Overregulation in the permitting process** creates lengthy timelines and stifles cable-laying ability. This increases costs, raises the risk of accidental damage, and prolongs any damage because companies are not able to incorporate sufficient resiliency or to rapidly deploy replacement cables in the event of a disruption.
- **Not having a dedicated minister of defense** contributes to a lack of resources and attention that leaves defense capabilities underfunded and overlooked. Defense responsibilities are instead carried out by the minister for foreign affairs.
- **The lack of a comprehensive national security or maritime security strategy** further complicates a coordinated response. However, this is gradually changing with the emergence of new institutions, the development of strategic frameworks, and a growing recognition that Ireland's island geography no longer guarantees protection.

Policy Recommendations

Ireland needs more vigorous and committed investment across key areas—technological, naval, and strategic—to build the capacity required to protect critical infrastructure and assert its role in regional and global security frameworks. In this regard, Dublin might consider several policy proposals:

1. **Preserve neutrality while bolstering security.**

Ireland's defense capabilities have been historically underfunded and insufficiently prioritized. Strengthening these capabilities is essential to protect critical infrastructure, including subsea cables, and to respond effectively to emerging security threats. The country can maintain its neutrality but may need to increase its defense capabilities to demonstrate credible deterrence. Ireland should adopt new policies, invest in these capabilities, and—within the scope detailed in this paper—ensure the protection of its maritime domain.

In this regard, Ireland should prioritize articulating an effective national security strategy, inclusive of the maritime strategy currently under development, to address challenges and find ways to improve the delivery of the security forces. In March 2025, the Taoiseach—the prime minister of the Republic of Ireland—established a new **Ministerial Council on National Security**, a productive step toward coordinating efforts across security agencies.

To meet these goals, Ireland should focus on building its navy by recruiting more personnel so it can staff more active naval vessels able to respond to incidents. These efforts may take time and require significant resources, as the INS currently faces challenges such as a limited fleet, a lack of helicopters, and ongoing difficulties in retention due to long deployments and low public appeal. Enhancing the navy's brand, improving working conditions, and offering competitive salaries could help attract and retain talent. In parallel, investments in autonomous drone technologies, such as unmanned underwater vehicles (UUVs), can bolster surveillance over Ireland's vast EEZ.

2. **Increase subsea cable redundancy.**

As it did in its National Cyber Security Strategy of 2019, the Irish government needs to continue to emphasize subsea cables as **critical infrastructure** to ensure sufficient funding, regulatory clarity, and greater investment in the INS, detection technologies, and other associated capabilities. To enhance resilience and reduce strategic vulnerabilities, it should encourage the development of more geographically diverse subsea cable routes and establish additional landing stations. This would help distribute risk, improve network redundancy, and strengthen Ireland's position as a secure hub for global connectivity.

Redundancy builds resilience: If one or two cables out of many are cut, traffic can be rerouted through neighboring fiber-optic paths. However, if a greater proportion of cables break, whether accidentally or intentionally, the remainder would not be able to accommodate all traffic, and entire regions might be knocked offline. Irish waters are vast—the Atlantic even more so—and cable breaks happen regularly, so redundancy is already necessary as the oceans cannot be patrolled and protected from every ship and wave.

Governments and the private sector can work together on this to enhance system resiliency. By accelerating permitting timelines and streamlining overly burdensome bureaucratic processes, such as multiyear environmental reviews, companies can lay more cables more quickly. Likewise, in incidents where cable repair is necessary, companies should be able to act immediately, especially in crisis scenarios, and they cannot be expected to wait overlong after a cable break for secondary permissions to begin their repairs.

Ireland would benefit from empowering MARA as the lead agency on subsea cables, establishing a clear and coordinated one-stop shop model. Doing so would also require clearly delineating how naval forces can support MARA in enforcement roles, including their legal authority, operational protocols, and resource sharing. The Irish government should also improve transparency and consistency in its licensing processes for subsea infrastructure. Conflicting interpretations—such as the UNCLOS suggestion that **no license is required** versus the claim by Irish national authorities that a license is indeed needed for cables crossing the EEZ—create regulatory uncertainty and risk reputational damage. Clearer guidance and streamlined procedures are essential to attract and retain investment in this critical sector.

The Irish state should take a more proactive role in coordinating environmental permitting and spatial planning for maritime infrastructure. A comprehensive state-led strategy would help prevent conflicts between competing seabed uses—such as fiber-optic cables and offshore wind farms—and ensure the sustainable development of Ireland's maritime domain.

3. **Create a database of incidents.**

Ireland should establish a comprehensive database of subsea cable damages to track the type of incidents, identify patterns, and support a more targeted approach to protecting infrastructure. This would reduce the signal-to-noise ratio by making it easier to identify which cables were cut by accident and which were damaged intentionally.

To reduce accidental damage, cable locations should be advertised to fishermen and commercial vessels so they can avoid these areas or exercise increased awareness when traversing them. Fostering stronger ties with the fishing industry could also enhance surveillance, as fishermen could help identify potential threats and suspicious activities. In addition, legal instruments might be strengthened to criminalize subsea cable sabotage.

4. **Engage in greater collaboration with allies.**

On a broader scale, Ireland should work closely with the United Kingdom and aligned states in Europe. Just as a rising tide lifts all boats, everyone would benefit from improved information sharing and investments in cable protection technology, including advanced sensors and monitoring tools. The European Union might allocate defense funds for developing new protection technologies, investing in cable repair capacities, and establishing joint naval missions to safeguard cables in the Baltic, Irish, Mediterranean, and North Seas. Ireland's EU presidency next year presents a major opportunity to organize EU-level maritime security conferences, potentially promoting collaboration with NATO and the United States to advance cable protection, information sharing, and joint workshops. To establish a recurring platform for collaboration, Ireland should consider hosting a yearly Valentia Conference, or some similar platform, on subsea security and infrastructure protection.

Ireland's recent partnership with NATO under the **Individual Tailored Partnership Program**, valid until 2028, grants greater access to NATO resources, including intelligence, and improves military preparedness to protect subsea infrastructure. Further cooperation with NATO—such as through the **Maritime Centre for the Security of Critical Undersea Infrastructure** and the **Baltic Sentry** military exercises—would help secure subsea cable supply chains and strengthen Ireland's maritime security. The country could explore establishing a joint expeditionary force initiative in Irish waters, modeled on existing NATO collaborations in the North Sea, and work toward more integrated data collection with NATO systems to allow for real-time sharing of maritime surveillance. It should also continue its participation in scenario-based simulations and tabletop exercises with the **European Centre of Excellence for Countering Hybrid Threats** in Helsinki to explore the potential impacts of cable disruptions and inform future strategies.

Furthermore, Ireland could receive training from allies such as the United States to strengthen its military capabilities and protect subsea infrastructure. Washington could provide technical support for monitoring Dublin's maritime domain through advanced submarine detection tools such as acoustic sensing and seabed surveillance technologies. Establishing a dedicated U.S.-Ireland security conference could also help deepen bilateral ties and promote strategic dialogue.

Most importantly, the United States could leverage its position as Ireland's largest source of FDI to encourage stronger protections for maritime and digital infrastructure. The continued presence of U.S. MNCs depends not only on economic incentives but also on Ireland's ability to project institutional stability, competence, and reliability. Without a deliberate effort to foster external confidence and demonstrate capacity in safeguarding critical infrastructure—or if broader political and trade disputes disrupt U.S. FDI in Ireland—MNCs may begin to shift future projects and investments to other countries. A resulting decrease in Irish tax revenue would consequently pose a challenge to proposals to increase military spending and build resilience, both financially and politically, further hindering the country's projection of security.

5. **Increase coordination with the private sector.**

Fostering closer collaboration with industry, including unambiguous communication about roles and processes in the event of cable damage or sabotage, is critical for Ireland and the world. Clear timelines and demands from the regulatory framework for building and maintaining subsea cables incentivize investment in the sector, which is the most surefire way to generate redundancy and therefore resiliency in subsea cable systems.

Creating a public-private platform of engagement could facilitate regular meetings and cooperation between these actors, which, as the **NATO 2030** initiative underscores, is important to address security challenges. In addition, government and industry leaders could organize an annual conference on public-private cooperation in subsea security to strengthen partnerships and harmonize regulatory frameworks.

At the same time, policymakers could increase cooperation with U.S. tech companies to ensure greater responsibility in supporting cable protection. They could, for example, require continuous monitoring as part of insurance agreements, regularly assess the infrastructure for potential threats and damage, or incentivize companies to invest in detection technologies to enhance the security of subsea cables.

Conclusion

Maritime infrastructure plays a pivotal role in Ireland's economy and national security, encompassing critical elements such as offshore wind farms (vital for retaining MNCs and supporting data centers), subsea cables, and electricity interconnectors. Over the years, the national focus on maritime issues has evolved significantly. While historically concentrated on fishing, there is now a growing recognition that the sea is a crucial asset for Ireland, both in terms of energy security and telecommunications. The country's strategic geography, disconnected from continental Europe, was historically considered a source of protection, but no longer offers the same security benefits in this new era of geopolitics. As the need for greater self-sufficiency becomes more pressing, it is clear that Ireland faces a substantial capacity gap in effectively safeguarding these essential infrastructures. Addressing this gap is vital to ensuring the long-term resilience of its maritime and energy sectors. ■

***Romina Bandura** is a senior fellow with the Project on Prosperity and Development at the Center for Strategic and International Studies (CSIS) in Washington, D.C. **Thomas Bryja** is a program manager and research associate for the Project on Prosperity and Development at CSIS*

This report is made possible by the generous support of the Smith Richardson Foundation (SRF).

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).