IIEA
Sharing Ideas
Shaping Policy

Another 'Twist' on Subsea Cable Repair: Developments in Europe and what role, if any, for Ireland

Camino Kavanagh

Table of Contents

If technology was about magic, it was also about brutal reality. The grapnel had to be lowered by chain and rope. A snapped chain could take a man's head off. A slip could be disastrous. Everything had to be carefully calibrated. All the directives were clear. The men remained on the one radio channel. Grapnel down. It hardly made a splash. Ten metres. Slowly it uncoiled on the winch. Fifty. One hundred. Past the twilight zone where no upper light could ever go. Two hundred. They followed the descent on the screens in the control room. They had mapped the currents. One kilometre. Two kilometres. It took an hour or more to descend through the waters. Three kilometres. Grappling in the dark. Four.

Twist, Colum McCann

Executive Summary

The security and resilience of critical undersea infrastructure have become prominent issues in European policy debates. Scores of articles and opinion pieces have also been penned on the topic – on cable damage in particular – yet far less analysis has ventured into the topic of repair, and its role within the broader security and resilience framework.

This paper provides an overview of recent industry analysis of the subsea telecommunications cable repair eco-system alongside evolving EU and national policy discussions on the topic. Drawing on recent expert reports, it discusses repair-related trends, and how repair is considered in the EU context and in Ireland more specifically. It highlights key challenges specific to the industry, Europe and Ireland, and explores how companies and countries are addressing them amid growing geopolitical and national security concerns. It also discusses some of the key issues that governments would need to consider and coordinate with industry and with connected countries should a reasonable worst-case scenario present itself. The paper concludes with a set of options for Ireland, some of which chime with recommendations the European Union has set out for Member States in recent policy directives, strategies and plans, and some of which chime with recommendations of the International Advisory Board on Subsea Cable Resilience, an initiative jointly led by the International Telecommunications Union (ITU) and the International Cable Protection Committee (ICPC). The findings of the paper are not intended to be definitive, but rather to stimulate much-needed discussion on the complex topic of repair

Ireland's dependence on subsea telecommunications cables is well documented, as are associated threats and vulnerabilities. While this situation presents clear risks, it also creates a strategic opportunity for Ireland to cooperate more closely with cable owners and operators, key maintenance and repair stakeholders and other governments to ensure an efficient and resilient repair eco-system, responsive not just to business and national security interests, but also to those of the broader public.

About the Author

Dr Camino Kavanagh is a Fellow with the UN Institute for Disarmament Research (UNIDIR) and a visiting Senior Visiting Fellow with the Dept. of War Studies, King's College London. Her current research focuses on international security, geopolitics, conflict and technology, with a specific focus on cybersecurity and critical subsea infrastructure.

Amongst other, Camino serves as a Senior Advisor to the UN Department of Political Affairs' Policy and Mediation Division on digital technology and conflict. She previously served as advisor and rapporteur to the UN negotiating processes on cyber/ICT and international security (the UN GGE and UN OEWG). Over the past decade, she has also worked with the Office of the UN Secretary-General and a wide range of UN entities, regional organizations, and government departments and agencies on issues related to digital technologies, national and international security, conflict, and diplomacy. She actively participates in several Track 1.5 and Track 2 initiatives in these fields.

Prior to this, Camino spent over a decade working in conflict and post-conflict contexts, including UN peacekeeping operations and political missions.

Acknowledgements

The author would like to express her appreciation to those representatives from the submarine cable industry, government and the business and research communities who provided insights and feedback on different iterations of this paper, and to the Institute for International and European Affairs for agreeing to publish it.

Introduction

Government interest in the security and resilience of subsea telecommunications cables has increased significantly over the last decade. In the European and transatlantic context, the Nord Stream pipeline explosions and published details of faults on submarine cables have accelerated such concerns, which now spread across the entire subsea cable eco-system.[1] The capacity to ensure timely repairs of subsea cable systems in complex situations is one such concern, including in Ireland, and is the topic of this paper.

The paper provides an overview of recent policy discussions relevant to repair in the EU context; differing perspectives on the need for additional repair vessels to service the region; and the relevance of such discussions to the Irish context against a background of growing external pressure on Ireland to protect the infrastructure in its waters. It puts forward different options for Ireland regarding repair. These options – all of which would require public entities investing in or partnering with industry and business – are not without their complexities and are highly dependent on the unfolding security context, in turn requiring a significant appetite for risk as well as significant coordination with industry and other actors. In addition to immediate-term recommendations on establishing a single point of contact within government on subsea infrastructure as well as a standing subsea infrastructure technical body to advise government on security and resilience-related issues, the short- and medium-term options include establishing a spare parts/ supply depot in Ireland; investing (or co-investing) in existing maintenance arrangements; supporting EU-backed calls for adaptable repair modules deployable on existing vessels for emergency, near-shore repair operations; converting a midsize vessel for hybrid repair operations; budgeting for regular exercises that align with national preparedness and maritime security strategies and plans; and investing in skills development and professional training in Ireland. Many of these speak to issues highlighted by the EU in its recent Action Plan on Cable Security and Submarine Cable Security Toolbox, and by the joint ITU-ICPC initiative on subsea cable resilience.[2] However, their viability in the Irish context requires much deeper exploration by relevant stakeholders, for which several core considerations such as existing industry maintenance arrangements, national strategic value, public interest, cost, integration with national and regional strategies (e.g., maritime security, cybersecurity), and plans (e.g., emergency preparedness) are presented.

Background: Repair and the European Context

As is widely known, most cable faults arise from either human activity such as fishing and anchoring[3] or natural events such as earthquakes and volcanic eruptions but recently there has been a marked uptick in reported antagonistic activity involving states posing risks to the infrastructure. This is particularly acute in certain maritime regions such as the Baltic and North Seas, the North Atlantic, the Red Sea and the South China Sea. Conversely, the number of reported annual faults -- approximately 200 -- has remained steady over the past two decades. This despite the number of kilometres of fibre optic submarine cables growing from approximately 1 million km in 2014 – to around 1.6 million km by 2025 – showing a statistical decline in the fault rate.[4] Nonetheless, given the current geopolitical and security context, governments in some regions - Europe in particular - are questioning whether current cable maintenance arrangements remain fit for purpose, with their concerns often at odds with those of the subsea cable industry.

According to a recent industry report, the number of subsea telecommunication cable kilometres is expected to increase by 48% by 2040.[5] The drivers of this expansion include AI adoption and the demand for cloud services, including the more recent focus on sovereign cloud solutions. Additional redundancy requirements, too, contribute to cable kilometre increases. Meanwhile, important architectural factors and technological advances - increased fibre pair count, repeater spacing, branching units, open cable systems and data centre and cloud compatibility – are all forecast to meet new digital demands and improve resilience of the infrastructure.[6]

Despite the increase in cable kilometres, annual repairs on newer cables are anticipated to increase by only 36% in the same period.[7] Moreover, by 2040, almost half of all vessels in the global cable fleet will be nearing the end of their approximate 40-year service lifespan,[8] an issue particularly pronounced for cable maintenance vessels, 64% of which will reach this milestone in the same period.[9] Sporadic investment in new vessels (only some 20 ships were built over the past decade) and the prevailing trend to adapt used or second-hand vessels (70% of said 20 vessels are conversions) to the maintenance fleet is reportedly a product of "*high capital costs, market uncertainty and maintenance agreement economics.*"[10] This investment pattern contrasts markedly with the substantial investment in cable infrastructure over the same period. The Asia region is where most vessels investments have been made and where additional vessel requirements are reportedly most needed, due to higher damage incidents.[11]

The same report notes that ensuring the resilience of the global cable network requires substantial and timely investment in the cable maintenance fleet. The future of the sector is contingent on "*balancing commercial viability, operational efficiency and increasing demands to ensure resilient, secure submarine cable infrastructure*".[12] It estimates

that an investment of roughly USD $3 billion is required to address vessel maintenance, replacement and expansion needs in the coming years.[13] A range of direct and indirect factors — CAPEX, design, finance, timeframe, fixed costs, OPEX, longevity, shipyard supply and demand, availability of specialised cable equipment — will influence investment decisions, including on whether to invest in new builds or in conversions. Conversions have always been a significant component of both the installation and repair fleets), although the costs of these are also increasing.[14]

Industry assessments of needs and risks contrast significantly with those of governments. Industry resilience preparedness generally responds to trend assessments of the most common causes of damage to the systems. According to International Cable Protection Committee (ICPC) data, there are on average, some 200 cable faults per year, and, as noted, that figure has remained static for some time.[15] In fact, the most common causes of damage to today's fibre optic systems are not overly dissimilar to those presented at the 1882 Paris Conference, the negotiations of which cumulated in the adoption of the 1884 Convention on Submarine Telegraph Cables as well as many of the submarine cable provisions in the UN Convention on the Law of the Seas (UNCLOS).[16] In the narrower European context, a recent EU report notes that the number of faults has been on the decline by 7% year-on-year.[17] This trend is accentuated in Northern Europe, where the volume of faults has decreased by 29% year-on-year since 2020. This decline in submarine cable faults is attributed to improved engagement with the fishing community, enhanced cable-laying standards implemented by companies, and improvements in route engineering and in cable design. It is also attributed to the decommissioning of two specific submarine cables (the TAT-14 and SEA-ME-WE 3), which were in shallow waters with most faults occurring in areas of high-density fishing and shipping activity and in mobile seabed conditions.[18]

Current industry assessments of cable damage, repair times, and new vessel investment needs do not necessarily highlight specific European maritime basins as requiring urgent attention from a maintenance perspective. Rather, new regulatory requirements, in turn driven by the national security concerns of governments, or other policy priorities such as marine spatial planning for offshore renewable energy development, might well pose a bigger barrier to repair.[19] Conversely, given the current geopolitical and climate context, governments across the region are increasingly compelled to ensure their preparedness postures now cover reasonable worst case risk scenarios such as the effects and consequences of extreme weather events and the actions of hostile actors in crisis or conflict. In this regard, many governments view the limited investment in maintenance vessels by vessel operators and system owners as an important vulnerability requiring mitigation

This issue of investment (or lack thereof) is confirmed in the aforementioned report by Infra-Analytics and Telegeography, which highlights that while there is still overall satisfaction with the current commercial maintenance models – i.e., the Consortium Zone (or 'club') and Private Maintenance Agreements – there are concerns with "*capabilities of the repair fleet and its long-term effectiveness and sustainability"*[20] In addition, the report notes that while competition for maintenance services is still seen in a positive light, it also raises concerns about "*price pressures and the financial challenges associated with deploying capital for new vessel investment*".[21] Moreover, the number of vessels available for maintenance is market driven, so a decline in the number of repairs means there are less incentives for maintaining the same or increasing the number of vessels. However, this might change in certain regions such as Europe, as governments are increasingly compelled to plan for high-impact, low-probability scenarios. The UK government, for instance, is currently assessing options following a parliamentary hearing on subsea cable resilience and preparedness that recommended it acquire a sovereign repair ship by 2030, leased to industry during peacetime, but made available for government in times of crisis.[22]

While the European Commission acknowledges that existing repair arrangements and vessels "*have proven effective to repair damaged cables with reasonable response time*",[23] it nonetheless suggests that the current number and capacity of repair vessels would be "*insufficient to timely intervene in case of systematic and simultaneous attacks to critical cables across different maritime areas of the European Union*".[24] It further stresses that maintenance and repair vessels are "*a major bottleneck for the capacity to recover from an incident*" and raises concerns about the availability of repair equipment and specialised workers across subsea sectors, an issue well-known to industry and which it is trying to address through different initiatives.[25] Several non-EU countries share similar concerns about specialised workers (engineers in particular) and the current challenges posed by an aging workforce. Many of these concerns are also articulated in defence-related strategy documents.

Dependency concerns are another important driver of government interest in investment in repair, with ever more countries of the view that relying solely on private or foreign-flagged repair companies is creating strategic vulnerabilities. Indeed, references to sovereign repair capabilities and capacities are increasingly evident in policy documents, generally referring to ownership of, or guaranteed access to repair vessels, targeted regulations, crew nationality and operational readiness. Each of these points leads to additional questions though, such as how governments would finance the vessels and sustain the high cost of idle ships; how key operational needs would be met, including with regard to the

maintenance of an experienced and skilled crew; and how jurisdictional issues such as guaranteed access to spares, and the permissions and liability arrangements necessary to undertake repairs on privately-owned submarine cables would be addressed.

A Cable Security Action Plan published by the European Commission in February 2025 suggests a range of actions aimed at strengthening the security and resilience of subsea infrastructure. These actions more or less cover the full resilience cycle, including maintenance and repair and the question of dependencies.[26] For instance, in the short term, the Action Plan suggests "*pooling budget from Union funding programmes to finance an increase in EU cable vessels capacities, as well as modular repair equipment*" that can be fitted onto non-specialised vessels, likely for shallow water or contingency repairs.[27]

In the medium term, should the need be identified, the Commission proposes building "*an EU Cable multipurpose Vessels Reserve ready to use, possibly through an Implementing Act under the Union Civil Protection Mechanism (including rescEU) (…) and complemented by regional framework agreements to secure the immediate availability of appropriate vessels with specialised crews*".[28] The latter would be used in emergency cases and would be capable of operating in harsh environments, although the Action Plan is silent on how this reserve capacity would interact or integrate with the existing cable repair eco-system, and on the finer detail of how it would be operated and maintained on a daily basis. A final recommendation is to "*design a joint approach to ensure the security of supply of cable spare parts through, for instance, targeted stockpiles*".[29] Following from the Action Plan, the Commission established an informal Submarine Cable Infrastructure Expert Group comprised of government authorities and ENISA,[30] which produced a first report in October 2025 mapping cable-related risks and proposing a set of stress tests as guidance for member States, several which relate to maintenance and repair.[31]

In January 2026, the EU Submarine Cable Infrastructure Expert Group published a second report which includes a Cable Security Toolbox of mitigating measures,[32] and a draft list of Cable Projects of European Interest (CPEI).[33] It also advises on maintenance and repair capacity for submarine cables.[34] Presented as a strategic measure, such advice on maintenance and repair is accompanied by a number of practical actions, which together connect to identified CPEIs and the risks identified in the October 2025 report. The launch of the report was accompanied by a first-of-its-kind EUR 20 million call under Connecting Europe Facility (CEF) Digital for "*cable repair capacities*,"[35] itself connected to the EU's intent of establishing Regional Cable Hubs to enhance information sharing and incident detection across the EU.[36] The expectation is that the adaptable repair modules would enhance operational repair capacity and provide an emergency response capacity when the Hub identifies such a need, or another entity has declared an emergency. This first cable repair capacities call will "*finance cable repair modules for use in the Baltic Sea in emergency situations*" [37], although a further call for other maritime basins is expected in 2026.[38] None of these documents discuss the significant challenges of modularisation on vessels not originally designed as cable ships. Nonetheless, the funding call delves deeper into some of the characteristics and requirements that applicants would need to meet.[39] The launch of these latest EU instruments came just days after an International Advisory Body on subsea cable resilience jointly led by the International Telecommunications Union (ITU) and the International Cable Protection Committee (ICPC) presented a series of recommendations, including on repair, many of which chime with those laid down in the EU Cable Repair Toolbox of Mitigating Measures.[40]

For its part, the Commission's Maritime Industry Strategy, currently under development, will likely include a focus on the maintenance sector, and the possibility of availing of the region's "*highly advanced industrial capabilities in building specialised vessels to maintain and repair submarine cables*".[41] Meanwhile, some individual countries are conducting market studies to determine whether they need to invest in sovereign repair capabilities or partner with industry to that end.[42]

Industry has generally pushed back on the sovereign capability question, notably where the purchase of new vessels is concerned, suggesting that governments should instead invest in strengthening the existing maintenance sector where a need has been identified, including through public-private partnerships. Some industry actors have also voiced concerns that government intervention by means of direct investment in existing maintenance companies may exacerbate the existing "*concentration risk*".[43] Instead, notes one commentator, governments should use their leverage to require long-term solutions involving multiple independent suppliers.[44] Some governments are listening, although they would likely peg any investments or interventions to a guarantee of some form of influence over how repair operations are prioritised in the event of multiple breaks affecting more than one jurisdiction, which in turn would require significant regulatory and licensing coherence and diplomatic engagement between connecting countries, as well as more robust cooperation with cable operators. For most coastal or island countries, this would represent an entirely new area of engagement that they are currently ill-prepared for.

Governments increasingly view key companies in the maintenance eco-system as critical assets. For example, France presents its "repurchase" of ASN, a company which operates two maintenance vessels as a highly strategic move. Singaporean conglomerate Keppel Ltd's recent acquisition of the UK-headquartered Global Marine Group, a company with a fleet providing global zone coverage, received positive reviews, although questions remain as to whether the new owners will overcome previous challenges regarding longer-term tonnage investment.[45] Moreover, it is unclear what the acquisition may mean for UK and broader European resilience in times of crisis. More recently, the EU Cable Security Toolbox takes on some of these issues, including the question of foreign ownership of cable maintenance vessels and depots by non-EU entities. More specifically, it proposes that these 'strategic assets' should be scrutinised and prohibited if controlled directly or indirectly by third states operating at odds with the security interests of the EU and member States. However, it does not clarify what this would refer to in practice.[46]

Technology may offer some solutions to real and perceived challenges relevant to current maintenance arrangements and for meeting precise needs in situations of crisis. The US Senate draft bill NDAA FY2026 pitched in this direction, specifically aiming to examine the feasibility of repairing 'covered cables' within 100 hours "*including through the development and use of aerial-deliverable, submersible, splicing robots*".[47] It would also look into the utility and practicability of developing 72-hour deployable portable cable landing stations.[48] The fact that these proposals did not make the final version of the Bill suggests they may just reflect innovative, if not wishful thinking, but they garnered attention, not least for their potential to disrupt existing maintenance arrangements.

As alluded to, the question of prioritisation,i.e., which cables are fixed first or which sector(s) should be prioritised in national (and EU) preparedness plans, is a current policy fixation, as are dependencies with other sectors, in particular energy. For industry, prioritisation of repairs remains largely a contractual issue linked to existing maintenance zone and private agreements. Some industry representatives suggest this would remain the case in a crisis, while others signal possible challenges regarding prioritisation that might arise when repair ships are flagged to other countries, even if such countries are traditionally like-minded.[49] In short, it is probable that government influence or control over such decisions may increase if certain cable systems (or segments thereof) are designated as critical infrastructure or as assets upon which essential national services or functions depend. There is important precedent for such action, especially in times of conflict.[50]

Several countries are also looking at strengthening cable repair capacities as well as including a possible surge capacity where cable maintenance, repair workforce and specialised skills are concerned in the event of crisis or conflict. The UK Strategic Defence Review's focus on 'specialist roles' such as engineering, cybersecurity and law in the envisaged reserve capacity is a case in point.[51] Even more so is the UK Parliament's recommendation that the Royal Navy stand up "*a cadre of reservists and serving personnel to learn cable repair skills on commercial repair vessels (…) to be called on in periods of heightened tension*".[52] In response, relevant government agencies have stated that they will work with industry to assess commercial cable repair capacity and determine the type of intervention needed. Their assessment will cover "*commercial capacity, educational and skills facilities and the potential benefits of establishing a cadre of commercial cable repair personnel with reserve characteristics*".[53] For its part, the EU Cable Security Toolbox recommends that Member State authorities "*develop technical training programmes to strengthen the skills of submarine cable repair teams*". This training would ideally cover advanced repair techniques and safety protocols, amongst other efforts.[54]

Several EU Member States, as well as Iceland, Norway, the UK and the US, are engaging industry stakeholders on many of these issues. In the EU context, the Submarine Cable Infrastructure Expert Group is hunkering down on implementing key elements of the Cable Security Action Plan and related instruments, including the aforementioned actions relevant to maintenance and repair. Meanwhile, NATO, too, is engaged in a range of Critical Undersea Infrastructure protection activity.[55] Its work on resilience, an increase in coordinated naval patrols, presence operations, regular exercises and enhanced maritime domain awareness, including in some instances to protect maintenance and repair operations, will help ensure some degree of deterrence-by-denial.

A Role for Ireland in Repair?

Ireland is highly dependent on subsea cables for international connectivity. It is connected internationally by some 14 subsea fibre optic telecommunications cables. The majority connect Ireland to the UK, four are transatlantic, connecting Ireland to the US, one also connects Ireland to Iceland and another to Denmark. Some are reaching their end-of-life cycle and need to be upgraded or replaced, while other new cable projects are in the pipeline (1 transatlantic cable, 3 new connections to the UK and another that will connect Ireland, France, Spain and Portugal). Ireland has an exceptionally large and important maritime and air area of responsibility. In addition to cables landing in Ireland, according to industry statistics, 58 percent of transatlantic [commercial] cables pass through the Irish EEZ.[56]

Ireland is viewed as a critical gateway for North American organisations looking to gain access to Europe (and Europeans' access to the US). Ireland is also one of Europe's major centre data centres, its strategic location rendering that transatlantic bridge all the more important. The future of the country's digital economy relies significantly on its ability to ensure direct connectivity between Europe and North America and secure and protect the infrastructure and data hosted on its territory and in its waters. However, factors, including Brexit, and over-reliance on UK-based international connectivity creates important vulnerabilities. Indeed, the EU Submarine Cables Expert Group has described Ireland's current connectivity situation as creating "*a single-point dependency that poses significant operational and security risks*" to both Ireland and the EU. As a result, the North Atlantic is highlighted as one of the priority areas for Cables Projects of European Interest (CPEI), defined as "*priority areas identified to enhance EU resilience, where private investment alone may not be commercially viable*" and potentially requiring intervention from the EU and/or Member States to cover funding gaps.[57] In this regard, new routes directly connecting Ireland with the continent (rather than going through England) are considered an important resilience measure, not least for ensuring uninterrupted connectivity, yet are still deemed to be insufficient. Therefore, building further redundancy directly connecting Ireland to other EU countries as part of a broader route diversity strategy involving both direct and branched connections to a variety of European states, and ensuring commensurate maintenance and repair capacities and capabilities will remain a priority in the coming years.[58] For Ireland, ensuring sufficient redundancy and continued availability of the cable systems across all their components is critical to sustaining existing, and attracting new, investment and, importantly, for meeting broader societal resilience needs. However, how the country can accomplish this is not straightforward.

First, the digital ecosystem itself is becoming increasingly complex, with layered and tiered dependencies operating on a global scale, in turn complicating resilience and emergency planning and response. Indeed, the fault characteristics of new highly complex cable systems directly connecting to cloud regions and other related infrastructure are still being clarified. Second, the current push to move to cleaner energy is producing new challenges on the seabed around the coast of Ireland, with high-density activity relating to the development of wind farms and inter-connectors, as well as the laying of new optical cable systems already underway. With the new regulatory body MARA now established, significant emphasis is being placed on marine spatial planning to ensure optimal segregation and separation and to avoid potential damage among different users. This spatial squeeze is requiring significant collaboration between MARA and other relevant authorities, particularly those responsible for fisheries, communications, the environment, security and defence.[59] Moreover, it increasingly requires exchanges amongst bordering countries. Third, geopolitical developments have increased concerns about intentional state-backed activity, including sabotage of or possible interference with the infrastructure (for pre-positioning purposes) or interdiction of maintenance/repair operations in or close to Irish waters, and their potential impact on the availability of the networks and systems the country and its neighbours rely on. These concerns tie in with those voiced in recent media articles about the country's ability to protect the infrastructure,[60] although such articles tend to be narrowly centred on the absence of naval capabilities rather than the gamut of agreements, cross-government actions, public-private coordination arrangements, capabilities, capacities and skills that small island nations such as Ireland need to put in place and invest in to protect such infrastructure. Nonetheless, recent developments, including an up-tick in significant climate events, the reality of conflict once again in Europe, growing incidents of suspicious activity involving foreign vessels in or near Irish waters, as well as significant uncertainty regarding the future direction and posture of the United States vis-a-vis Europe brings home the urgency of these issues.

Government responses to identified challenges, threats and vulnerabilities to subsea telecommunications cables (and other critical undersea infrastructure) are broad-ranging and set to increase. For instance, calls for the country to increase its capacity to police its waters have resulted in increases in defence expenditure, the purchasing of additional patrol vessels (the P60 fleet extension programme) and growing investments in maritime and subsea surveillance technologies (e.g., the recent multi-million contract with Thales DMS France for the provision of towed sonar array capability), as well as investments in related R&D.[61] The country has also increased its engagement with EU PESCO projects specifically focused on critical undersea infrastructure, and has increased its engagement on CUI, maritime security and cybersecurity issues under its Individual Tailored Partnership Programme (ITPP) with NATO. Much remains to be done, however, to meet expectations of Ireland's capacity to protect the infrastructure in and around its waters. The latter is a hotly debated issue, often tying into broader domestic debates on the country's historic under-investment in the Defence Forces and the question of the country's long-standing policy of military neutrality, and seldom tied to the actual resilience needs of the country.

The country's first maritime security strategy, launched in February 2026, is expected to be an additional enabler for meeting key security and resilience objectives, notably where identified human resource, capacity and capability gaps are concerned (e.g., those identified in the Commission on the Defence Forces' report[62] and in the current Programme for Government[63]). The protection of critical undersea infrastructure is a priority area for the Strategy, informed in no small part by the substantial input from civil society and industry on CUI in the public consultation that has informed the Strategy's development.[64] Much of this input has been centred on ensuring that security does not inadvertently undermine CUI resilience, rather that security and resilience are necessarily complementary.[65]

Ireland's eventual transposition of relevant EU instruments into national legislation (including the Network and Information (cyber security) Directive 2022/2555 (NIS-2), the Critical Entities Resilience (CER) Directive and the revised Cybersecurity Act (CSA2), including its targeted amendments to NIS2[66] should advance resilience efforts, notably on the cyber and supply chain security fronts, directly implicating the National Cyber Security Centre and relevant regulators, as well as a range of other Irish government departments and services from the Department of the Taoiseach through to Communications and Defence. Government-led market and EU Expert Group studies on cable resilience needs are already identifying priority areas for investment, including where redundancy is concerned. There are expectations that the Department of Communications' direct involvement in the EU Submarine Cable Infrastructure Expert Group will also ensure coherence of Irish government actions on resilience with EU objectives, and that the Department of Defence's engagement with the European Defence Agency and other regional entities ensures that Irish concerns and those of other Member States, including with regard to the cooperation and capabilities required to police Irish and contingent waters, are not only voiced but effectively addressed.

Recent agreements between Ireland and the UK, and between the EU and the UK include strong commitments to cooperate on maritime security, and on protecting critical undersea infrastructure.[67] Legislative bodies view that commitment as an important hook for more concrete action. Notable, for instance, is the British-Irish Parliamentary Assembly recommendation that the governments of Ireland and the UK establish a joint statutory Cables Protection Commission to protect and monitor critical infrastructure.[68] Comprised of government, defence and industry representatives, the body, if ever established, would be commissioned to map existing undersea infrastructure, establish monitoring patrols in Irish and British waters, and enhance resilience capacity.[69] Already, Ireland and the UK are working to implement their high-level political commitments on critical undersea infrastructure protection, and it is likely that such work will continue, if not intensify following the 2026 Summit involving the two countries. It would beggar belief if such cooperation did not cover issues pertinent to maintenance and repair of subsea cable infrastructure.

Both industry and academia have flagged important regulatory challenges that risk undermining other positive developments. This is particularly the case where repair of undersea cables is concerned. According to industry statistics, regulatory barriers to repair are increasing the time to commence repair globally, despite the lower number of repairs.[70] Furthermore, such delays can trigger service effects in other jurisdictions. In some instances, permits, authorisations or security guarantees can become bargaining tools a form of political leverage so to speak, creating significant delays for a repair operation. The Red Sea, a significant security and regulatory choke point, is a case in point.[71]

In Ireland, a long-standing status quo allowed cables to be repaired in the country's territorial waters (TW) via a simple notification procedure, while UNCLOS provides a basis for freedom to repair in the Exclusive Economic Zone (EEZ).[72] However, the 2021 Maritime Area Planning Act (MAPA) left it unclear whether a license would be required for conducting repairs in the country's EEZ. Beyond inconsistency with UNCLOS, this lack of clarity represented a major *faux pas* in the current geopolitical environment in which the timeliness of repair is of the essence. These challenges are nonetheless widely known and discussed within government and with industry, and both MARA and the Department of Communications have publicly affirmed that efforts are underway to address them. To wit, the Department of Climate, Energy and the Environment's recent circular to MARA clarifying that a maritime usage licence is not required to conduct emergency works for undersea cables and confirming that the Department will seek legislative remedies to further clarify the matter has triggered a collective sigh of relief amongst operators of subsea cable infrastructure.[73] Moreover, Ireland's recent experience in resolving the issue can be leveraged to inform EU and international cable diplomacy efforts to promote the removal of regulatory barriers to repair in other jurisdictions, a core recommendation of the ITU-ICPC led International Advisory Body on Submarine Cable Resilience.[74]

At present, the number of cable faults in Irish waters per year remains very low, with most recent damage incidents caused by trawlers and natural hazards (submarine landslides/turbidity currents). Exact data is not publicly available but according to industry sources, incidents of cable faults in Ireland's TW or EEZ are few and far between.[75] Publicly available industry trend assessments on time-to-repair and causes and types of cable damage do not necessarily highlight the North Atlantic region as an area requiring urgent attention in terms of maintenance needs, although current expansion trends indicate that there will be a need to meet minimum vessel requirements out to 2040.[76]

Conversely, governments across the North Atlantic, including Ireland, are on increased alert due to the suspicious activities of Russian special purpose vessels such as the Yantar and the so-called "shadow fleet". The EU and numerous individual countries have highlighted the risk of coordinated attacks affecting various systems and sectors simultaneously. A variation of such risk could include damage to several transatlantic cables resulting from a geological event at sea (an interesting precedent is the 1929 Great Banks earthquake and ensuing turbidly currents that knocked out some 12 transatlantic electric telegraph cables); cuts by a fishing trawler, intentional or otherwise (along the lines of the 1959 case in which a Soviet trawler was suspected of (although not held responsible for) cutting several AT&T transatlantic

cables); or denial of access to a repair ship or to a spares depot. Other scenarios include loss incurred from a direct or indirect cyber-attack affecting remote management systems and other control systems; backdoor access to a system; a cyber or PNT attack affecting a repair vessel's operations; or a cyber-attack targeting the OT systems of a co-dependent sector such as energy. Variations of these scenarios and related escalatory stages figure in the EU's recent report and recommendations on risk mapping and stress testing.[77]

Cables connecting to Ireland or passing through or close to its waters are owned and operated by companies that are part of the Atlantic Cable Maintenance zone Agreement (ACMA), or private maintenance agreements such as the Atlantic Private Maintenance Agreement (APMA), which, to date, have provided efficient and effective maintenance services. Moreover, transatlantic communications are generally resilient -- with a low probability of total or significant loss of the systems and significant redundancy to push traffic elsewhere (if that "elsewhere" is not also affected). However, as noted in the UK 2025 National Risk Register, should such a risk materialise, there is an expectation that it would likely be impactful, even when redundancy and alternative back-up systems are in place.[78] The re-routing and recovery demands would likely overwhelm the sector, at least temporarily. In a situation of crisis or conflict, the timeframe would evidently be much longer. Indeed, it is unclear -- at least publicly -- how cable repairs would be mobilised and prioritised in such a situation. Governments would need to have a good grasp of contractual arrangements under existing maintenance agreements which already cover elements of prioritisation. They would need to ensure channels for coordination amongst themselves and with maintenance/repair operators. They would need to ensure that national regulatory frameworks provide nimble access to vessels for timely repairs. They would also need to ensure greater capacity for investigating the cause of damage, for which coordination with industry and other countries is essential.

For Ireland, such a scenario presents important challenges. The government is working with industry and the EU to ensure sufficient redundancy through additional systems and alternative sources, and it has clarified the regulatory ambiguity around whether operators need to obtain a license for emergency repairs. Yet, like most countries, Ireland exercises no influence over the actual maintenance zone and private maintenance agreements, which are ultimately market-driven. This has not been a challenge to date. However, should a worst-case scenario present itself or an extended crisis prevail, the options for timely repair outside a business-as-usual scenario in which extant processes are followed remain unclear. Indeed, in business-as-usual cases, governments play a largely supportive role, if any at all. However, in circumstances where the safety of a vessel or its crew is compromised, or where insurance is invalidated due to elevated risks or an active conflict, government roles and responsibilities would change. These roles and responsibilities – and the enabling agreements, policies, capacities and capabilities – would need to be clearly defined, planned and budgeted for. A range of other challenges would also need to be considered including access to spares and a number of other supply chain questions. In addition, there are questions concerning the number of procedures and mechanisms related to incident detection and response, and inter-agency, inter-governmental and public-private coordination which would also need to be in place.[79]

Needless to say, the EU Cable Security Action Plan, the recently published Cable Security Toolbox, other relevant EU instruments such as NIS 2, CER, the proposed Cybersecurity Act (CSA2), recent political agreements with neighbouring countries, recent announcements of repair-related grants and tenders, growing assertiveness on the part of Irish government departments in shaping subsea cable policy, as well as the new maritime security strategy provide an important opportunity for greater clarity, coordination and action in this area.

Within this broad context, there are a few niche areas in the Irish context that merit more in-depth discussion for their potential high value for national, regional and transatlantic security and resilience in the short and medium-term. These would complement existing efforts to enhance redundancy and build resilience across extant and projected subsea cable systems and to upgrade Irish naval capabilities and emergency operations. Besides recommendations 1 to 3, which are long overdue and require urgent action, each of the subsequent options would merit a deeper assessment of their actual viability, not least since some would involve breaking into a highly specialised and high-cost sector and into deeply entrenched yet decently functioning maintenance arrangements. Most align fully or in part with actions laid out in the EU Cable Security Action Plan, with the recommended Strategic Measures (SM) and Technical and Support Measures (TM) identified in the EU Cable Security Toolbox and with the repair-related recommendations of the ITU-ICPC led International Advisory Body on Submarine Cable Resilience. Given the focus on and expectations of Ireland, the time is ripe for their consideration. They include:

Recommendations for the immediate term

1. **Establishing a single point of contact or entity within government** on subsea cable infrastructure for coordinating policy and action across the resilience, defence/security and marine spatial planning communities, and for engagement with industry and connecting countries on issues such as threat detection, stress-testing,

fault reporting, crisis management, incident response and repair. This could lay the ground for Option 6 below. Aligns with EU Cable Security Toolbox SM05, SM06, TM01 and TM04, ITU-ICPC WG1, Recc.1, 2, 10, 11]

2. **Establishing a standing technical body** for information-sharing and to advise the government on subsea cable infrastructure-related developments (regulatory developments, including progress on streamlining regulation; potential supplier concentration risks; resilience standards; cyber-physical security standards; inter-operability possibilities; technology and innovation). Aligns with EU Cable Security Toolbox SM01, SM02, SM05, SM06, TM01 and TM04; ITU-ICPC WG1, Recc.1, 10.

3. **Conducting regular exercises to stress-test restoration and repair of key undersea infrastructure in Irish and contingent waters with industry and connecting countries** to identify gaps or barriers - policy, regulatory, procedural, capability, operational - that could impede timely restoration of service and physical repair of the systems across different peacetime, crisis and conflict scenarios and escalatory stages. Aligns with EU Cable Security Toolbox SM02, SM05, SM06; ITU-ICPC WG1, Recc.11.

   Core considerations: national strategic value; public interest; mandate (inc. clear authorities for operating across scenarios; scope and basis for information sharing); coordination (intra- and inter-gov; industry); integration with maritime security strategy, cyber security strategy and national resilience and emergency planning; bi-lateral and regional cooperative agreements; readiness (vessels, equipment, infrastructure, logistics, interoperability); legal/regulatory barriers locations; scenario design and threat modelling; public communication/ outreach; future proofing.

Further options (short-term)

4. **Investing in current maintenance arrangements**, such as ACMA in the form of a public-private investment. Aligns with EU Cable Security Toolbox SM01, SM02, SM03, SM06 and TM04; ITU-ICPC WG1, Recc. 2, 6.

   Core considerations: national strategic value; public interest; integration/ alignment with national resilience/ emergency planning/ maritime security strategy; scope of investment/ membership terms (inc. prioritisation modalities in the event of unexpected, non-traditional events such as the ones discussed above); PPP structure; potential supplier concentration risks; governance/ influence in decision-making; financial commitments; integration with national capabilities; integration with potential pooling arrangements; legal/regulatory/ contractual issues; national CUI industry coordination mechanism; evolution/ future proofing of arrangements.

5. **Investing or co-investing in the establishment of a cable spares and joints depot** possibly in Cork, which boasts a deep-sea harbour, in line with the EU Cable Security Action Plan short-term recommendations on repair and EU Cable Security Toolbox SM02, SM03, SM04 and TM04; ITU-ICPC WG1, Recc.4, 6.

   Core considerations: sufficiency of current maintenance arrangements; *national strategic/ economic value; public interest; cost/financing arrangements; location and required infrastructure; standards, certification, and industry alignment; ownership/governance model; security; integration with national resilience and emergency planning/ national maritime security strategy; integration with existing maintenance arrangements; future proofing.*

Further options (mid-term)

6. Consider proposing Ireland as a **Regional Cable Hub** under the EU Digital Europe Programme as a means to enhance secure information sharing and emergency preparedness amongst relevant public and private actors, and to enhance detection of potential malicious activity. This would be an out-growth of Option 1 above. Aligns with EU Cable Security Toolbox SM05, SM06, TM01 and TM04, ITU-ICPC WG1, Recc.2, 10, 11.

   Core considerations: national strategic/ economic value; public interest; cost/funding/ procurement; Digital Europe Programme Call specifications;[80] regulatory barriers; workforce/skills; integration with national resilience and emergency planning/ maritime security strategy; integration into existing maintenance arrangements; integration with national capabilities; integration with potential pooling arrangements; future proofing.

7. **Refitting an existing nearshore vessel with modular repair equipment capabilities (**along the lines of the Commissioners of Irish Lights aids to navigation (AtoN) vessel, the ILV Granuaile) and/or s**upport relevant industry actors seeking EU funding under the Connecting Europe Facility for adaptable repair modules deployable on existing vessels for emergency repair operations.** Any vessel considered should be capable of

operating in difficult sea conditions and able to "receive the modules with minor adaptation and operational preparation" and meet other relevant requirements. Aligns with the EU Cable Security Action Plan short-term recommendations on repair and EU Cable Security Toolbox SM02 and TM04; ITU-ICPC WG1, Recc.4.

Core considerations: sufficiency of existing maintenance capabilities and arrangements; national strategic/ economic value; public interest; maritime conditions; vessel design/ suitability in accordance with CEF call specifications[81]; regulatory barriers; technical barriers ; cost/funding/ procurement; workforce/skills; integration with national resilience and emergency planning/ maritime security strategy; integration into existing maintenance arrangements; integration with national capabilities; integration with potential pooling arrangements; future proofing.

8. **Converting an existing mid-size vessel (e.g., from the PSV or OSV markets) into a repair vessel for both communications and energy cables,** in line with the EU Cable Security Action Plan's mid-term recommendations on repair and EU Cable Security Toolbox SM02 and TM04; ITU-ICPC WG1, Recc.4.

   Core considerations: sufficiency of existing maintenance capabilities and arrangements; national strategic/ economic value; public interest; regulatory barriers; technical barriers; standards (vis modular equipment and systems); governance/ownership; cost/funding/ procurement; cable handling capability; security; workforce/ skills; integration with national resilience and emergency planning/ national maritime security strategy; integration into existing maintenance arrangements; integration with national capabilities; integration with potential pooling arrangements; future proofing.

9. **Supporting the establishment of a specialised undersea infrastructure engineering centre of excellence in Ireland** that provides intensive training in specific areas to ensure the country has the human capital needed to protect and expand its critical subsea telecommunications and energy infrastructure sectors and can position itself as a European and/or transatlantic subsea engineering centre of excellence. This would be an important contribution to extant and projected work force demands in both sectors, as well as to contributing to building up a possible national and European emergency reserve capacity for critical undersea infrastructure protection in the event of crisis or conflict. Where fibre optic communications cables are concerned, such a centre could link into existing centres of excellence such as Global Marine's Cable Engineering Training College, as well as broader university programmes such as the Berkely Certificate in Digital Infrastructure or the upcoming University of Genoa (UNiGE) Master's Programme in Digital Subsea Infrastructure, both of which involve industry.

   Since no engineering training centre covering both undersea telecommunications and undersea energy infrastructure currently exists, the National Maritime College Ireland (NMCI), based in Ringaskiddy, Cork could be a home for such a centre of excellence and could be made available to civil and naval engineers in Ireland and beyond, as well as others seeking a career in the digital and energy sectors Such a centre would link up to emerging technology solutions as well as other important skills development initiatives already underway across Ireland. More intensive formats such as Symposia, summer schools and bootcamps could also be offered. Aligns with EU Cable Security Toolbox S02and TM04; ITU-ICPC WG1, Recc.9;

   Core considerations: national strategic/ economic value; public interest; sectoral demand/workforce planning; existing emergency retention initiatives and related challenges[82]; training scope and specialisation; location and infrastructure/ system requirements; industry partnerships/ academic collaborations; governance; funding and economic sustainability; integration with national resilience and emergency planning/ national maritime security strategy; global positioning and competitiveness (Global Ireland); future proofing.

10. **Supporting the establishment of a maritime security innovation and experimentation centre** involving key industry actors and Irish research institutes to test technological solutions in subsea and seabed security cases in the Irish maritime security context. Geographical focus could include high risk areas where there are currently important monitoring and surveillance gaps, as well as certain transit areas and all landing points for telecommunications cables and energy interconnectors and pipelines. Aligns with EU Cable Security Toolbox SM-02 and TM03.

    Core considerations: national strategic value; public interest; scope of activities; location/infrastructure; governance; research focus; industry/ academic partnerships; test ranges/ simulation systems + data policy; security/classification and regulatory/legal; cost/funding; skills and training; future proofing/ scalability.

11. **Sponsoring fellowship programmes, professional training programmes and vocational training/ apprenticeships** for new generations, including in the fields of photonics, subsea and marine engineering, international law and diplomacy. Aligns with EU Cable Security Toolbox SM 05, SM 06 and TM04; ITU-ICPC WG1, Recc.9.

    Core considerations: national strategic value; public interest; target groups/ programmes; integration into national workforce planning; academic/ industry partnerships; international cooperation; funding models; future proofing.

To conclude, protecting Ireland's critical subsea infrastructure is not about eliminating risk, but about developing national capacity to protect and deter, while maintaining the resilience to absorb disruption, enable timely repair, recover quickly, and adapt swiftly, regardless of the prevailing context. This is no easy task given the complexity of our dependencies on the systems, their cross-domain character, and the realities of an increasingly crowded and contested maritime environment. Strengthening relations with industry and prioritizing the topic of maintenance and repair is one step in that direction.

Endnotes

1. C.Kavanagh, J.Franken and W.He, Achieving Depth: Subsea Telecommunications Cables as Critical Infrastructure", UNIDIR, April 2025.

2. European Commission, European Parliament '.EU Action Plan on Cables Security', February 2025; 'Security and Resilience of Submarine Cable Infrastructures: Submarine Cable Security Toolbox and Cable Projects of European Interest', Submarine Cable Infrastructures informal Expert Group supported by Analysys Mason & Axiom, January 2026

3. See, for example, ICPC Viewpoint 'Damage to Submarine Cables from Dragged Anchors', 24 February 2025.

4. M. Constable, L. Burdette and A. Mauldin, 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies', Infra-Analytics and Telegeography, June 2025, pp. 2,30.

5. 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies', Telegeography and Infra-Analytics, June 2025.

6. 'The Four Forces Behind the Subsea Boom and Why They Matter', Subsea Cables Telecom Review, April 2025.

7. 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies', Telegeography and Infra-Analytics, June 2025, pp.3, 50.

8. The much-referred to '40-year lifespan' is not by design. It is mainly due to low margins in maintenance, making it very difficult to plan investment in newer vessels.

9. 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies', June 2025. Often newer vessels might start off in installation, but as they get older, they are moved to maintenance. This isn't necessarily a problem. For instance, the C.S. Cable Innovator was built to lay transatlantic systems for Cable & Wireless, but is now in the North American Zone Cable Maintenance Agreement (NAZ agreement) on standby for maintenance in the North Eastern Pacific Ocean - or the C.S. Sovereign which was purpose built by BT to be a versatile install/repair vessel, but later moved into dedicated maintenance. Maintenance doesn't necessarily need newer ships - but even older ships are expensive to buy/convert for maintenance purposes. Communication with industry rep. 17 December 2025.

10. Ibid (pp. 3, 4, 29-35, 55-73).

11. 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies', Telegeography and Infra-Analytics, June 2025, pp. 52, 59, 61, 63, 77, 97; A.Palmer-Felgate, 'Global Cable Repair Data Analysis, Edge Network Services Limited., ICPC Annual Plenary, Montreal, Canada, April 2025.

12. Ibid (p.3). Some 62 vessels are actively engaged in the installation and maintenance of subsea telecommunications cables. Owners with most vessels are ASN, SubCom, Orange Marine and Global Marine. Asia-based operators own 53% of the global fleet. Several companies operate only a few vessels. Some 26 vessels (42%) operate in the cable installation sector; 19 (31%) provide dedicated services for maintenance agreements. The remaining 16 vessels (27%) operate between installation and maintenance, with some providing ad-hoc services in the Baltic, Asia-Pacific and Americas regions. The maintenance fleet is generally older than installation vessels, reflecting the trend to repurpose ageing vessels from installation to maintenance activities. While the latter may well reflect investment challenges of the sector, converted vessels are usually configured for both installation and maintenance operations (p.55).

13. Ibid. p.2

14. For instance, the report assesses that the total capital expenditures necessary for new purpose-built vessels will range from $145-155 million for installation/multi-purpose vessels and $105-120 million for maintenance vessels. Total capital expenditure for OSV vessel conversions are assessed to have quadrupled in the last 5 years from $38 million for an actual acquisition in 2019 to $95-130 million for two vessels available in the OSV market in 2025. Ibid (p.67)

15. A.Palmer-Felgate, 'Global Cable Repair Data Analysis, Edge Network Services Limited., ICPC Annual Plenary, Montreal, Canada, April 2025.

16. The British delegation to the 1882 Paris Conference presented statistical data on the principle causes of damage to cables, dividing them into three categories: (1) natural causes (60%); (2) accidental or unintentional acts due to accidents at sea or force majeure (35%); and (3) intentional acts arising from malice or gross negligence (5%). These and other data informed the negotiations resulting in the 1884 Convention, which aimed to protect submarine cables from damage caused by activity such as trawling and anchor drag. L. Renault, *La Protection des Télégraphes Sous-Marins*, Octobre-Novembre 1882. Extrait de la Revue de Droit International, Librairie Europèene C.Muquardt. (p.16), cited in C.Kavanagh and J.Winkler, 'Continuities and Discontinuities: Subsea Cables and Geopolitics' (forthcoming 2026).

17. "Security and Resilience of EU Submarine Cable Infrastructures - Mapping, risk assessments, stress tests", Submarine Cable Infrastructures informal Expert Group supported by Analysys Mason & Axiom, October 2025.

18. Ibid.

19. 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies, p.15; U.S. joint Subcommittee on Transportation and Maritime Security and Cybersecurity and Infrastructure Protection hearing, "Securing Global Communications: An Examination of Foreign Adversary Threats to Subsea Cable Infrastructure, 20 November 2025; communications with industry reps. December 2025.

20. The maintenance agreements are geographically determined with repair ships operating from base ports across the globe. See 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies', pp.3-4 and 21-28.

21. Ibid.

22. Government response to UK Parliament Joint Committee on the National Security Strategy: Subsea telecommunications cables: resilience and crisis preparedness – Final Report, Appendix 2, 17 December 2025.

23. EU Action Plan on Cable Security, European Commission Joint Communication to the Parliament and the Council (Doc. 52025JC0009), February 2025.

24. Ibid.

25. See, for example, the Next Generation Programmes launched by ESCA and SubOptic, Several cable owners and operators are actively engaged on this topic

26. For a deeper discussion on resilience and subsea cables, see Kavanagh, Franken and He, UNIDIR 2025.

27. EU Action Plan on Cable Security.

28. Ibid, p.14

29. EU Action Plan on Cable Security.

30. For information on the Expert Group, see: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3940

31. 'Security and Resilience of EU Submarine Cable Infrastructures - Mapping, risk assessments, stress tests', Submarine Cable Infrastructures informal Expert Group supported by Analysys Mason & Axiom under service contract EC-CNECT/2024/OP/0070, October 2025.

32. The mitigating measures are somewhat predictable. Strategic Measures include: increasing redundancy, reinforcing EU maintenance and repair capacity and capabilities, reducing exposure to foreign vendors and operators, promoting manufacturing facilities, stocks and depots in the EU, implement and strengthen international regulatory and administrative measures on submarine cable protection, promote coordination between industry, Member States, NATO snd international bodies. For their part, Technical and Support measures include: ensuring adequate physical and cyber protection of submarine cables; reinforcing physical and cybersecurity as well as power resilience of dry plant facilities; increasing monitoring, surveillance and detection capabilities; and strengthening maintenance and repair capabilities. 'Security and Resilience of Submarine Cable Infrastructures: Submarine Cable Security Toolbox and Cable Projects of European Interest', pp.6-7.

33. Ibid, pp 28-52. The report proposes 13 CPEI areas grouped into three stages, each covering s 5-year period.

34. Ibid

35. See 'CEF-Digital new call open: €20 million to ensure fast emergency repair of submarine cables in the Baltic Sea', European Health and Digital Executive Agency (HaDEA), 05 January 2026, available at: https://hadea.ec.europa.eu/news/cef-digital-new-call-open-eu20-million-ensure-fast-emergency-repair-submarine-cables-baltic-sea-2026-02-05_en

36. Deploying Strategic Cyber Capabilities Across Europe (DIGITAL-ECCC-2025-DEPLOY-CYBER-09), Digital Europe Programme (DIGITAL), October 2025.

37. European Commission. CEF-Digital new call open: €20 million to ensure fast emergency repair of submarine cables in the Baltic Sea. February 2026. https://hadea.ec.europa.eu/news/cef-digital-new-call-open-eu20-million-ensure-fast-emergency-repair-submarine-cables-baltic-sea-2026-02-05_en

38. Ibid.

39. Submarine Cable Repair Capacities-Pilot Works (CEF-DIG-2026-CABLE-REPAIR-CAPACITIES-PILOT), Connecting Europe Facility, February 2026.

40. International Cable Resilience Summit, February 2026, https://www.itu.int/digital-resilience/submarine-cables/events/iab-deliverable/ For the recommendations of the Working Group on Timely Recovery and Repair, see https://www.itu.int/digital-resilience/submarine-cables/wp-content/uploads/sites/2/2026/02/IAB-WG1-Recommendations.pdf

41. European Commission, Open Call for Evidence: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14745-EU-industrial-maritime-strategy_en

42. Kavanagh, Franken and He, UNIDIR 2025

43. Input from industry representatives, February, 2026; See also, S. Jurnell, 'The Ticking Clock in Submarine Cable Repair – A Collective action problem'. LinkedIn blogpost, 20 February 2026.

44. Ibid.

45. Baird Marine 'Three blind mice, see how they run, part two: Global Marine Systems and Keppel [Offshore Accounts]', 19 March 2025.

46. Submarine Cable Security Toolbox and Cable Projects of European Interest, Strategic Measure 2, (4), p.8

47. Proposed bill - S. 2296: National Defense Authorization Act for Fiscal Year 2026, pp.903-909 (as passed by the Senate on Oct.9 2025)

48. Ibid.

49. UK Parliament Joint Committee on the National Security Strategy: Subsea telecommunications cables: resilience and crisis preparedness – Final Report (pp. 25).

50. C.Kavanagh, 'All Hands on Deck: Subsea Cable Repair in Crisis and Conflict' (*forthcoming, 2026*).

51. UK Strategic Defense Review 2025 (p.65)

52. UK Parliament Joint Committee on the National Security Strategy: Subsea telecommunications cables: resilience and crisis preparedness – Final Report. Recommendation, paragraph 75.

53. 'Government response to Parliamentary Committee report on resilience and crisis preparedness of subsea telecoms cables', 'Subsea telecommunications cables: resilience and crisis preparedness – Final Report', Appendix 2.

54. 'Submarine Cable Security Toolbox and Cable Projects of European Interest', pp. 16, 21; C.Kavanagh, 'All Hands on Deck" Subsea Cable Repair in Crisis and in Conflict' (forthcoming, 2026).

55. C. Kavanagh, 'Wading Murky Waters: Subsea Cables and Responsible State Behaviour', UNIDIR 2023; Kavanagh, Franken and He, UNIDIR 2025.

56. Communication with ICPC representative, 03 December 2025.

57. Prioritisation under CPEI includes not just the cable build (procurement and installation) but also enhancing maintenance and repair capabilities. 'Submarine Cable Security Toolbox and Cable Projects of European Interest', p. 22.

58. Ibid. One such route is the Ireland to France, Portugal and Spain cable – the PISCES project – expected to be operational in 2027/2028. Another is the Celtic-Interconnector, which while a power cable, is expected to also integrate a direct fibre-optic connection between Ireland and France. (p38). Input from industry representative, February 2026.

59. Valentia Island Symposium 2024, Report of Proceedings. Kavanagh *et al*.

60. Webber, J, 'How Ireland became the weak spot in Europe's Defences', *Financial Times*, 25 November 2025.

61. 'Minister for Defence launches €1.7 billion Defence Sectoral National Development Plan 2026-2030', Department of Defence, 11 December 2025.

62. See Commission on the Defence Forces, 'Report of the Commission on the Defence Forces,'February 2022

63. See Government of Ireland, 'Programme for Government 2025.' January, 2025

64. Address by Dr. Margaret Stanley to the Joint Committee on Defence and National Security on the Department of Defence's work to prepare the National MARITIME Security Strategy, October 2025.

65. Communications with industry reps. December 2025

66. See European Commission, 'Proposal, for a Regulation for the EU Cybersecurity Act' and 'Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act', 20 January 2026.

67. See 'Statement released by Prime Minister Keir Starmer and Taoiseach Micheál Martin on 6 March following UK-Ireland Summit', 6 March 2025; and "Security and Defence Partnership between the European Union and the United Kingdom of Great Britain and Northern Ireland" (Document 8709/25), and related "EU-UK Summit 2025 -Joint Statement" (Doc. 8245/5/25), Council of the European Union, 19 May 2025.

68. British-Irish Parliamentary Assembly, Committee B (European Affairs), "UK-EU Defence and Security Cooperation Post-Brexit – Final Report", October 2025, p.12

69. Ibid.

70. A. Palmer-Felgate, 'Global Cable Repair Data Analysis', April 2025.

71. 'Valentia Island Inaugural Symposium on Subsea Cable Security and Resilience', 12-14 October 2024.

72. See specifically Article 58, United Nations Convention on the Law of the Sea. Ireland ratified UNCLOS in 1996.

73. Department of Climate, Energy and the Environment, Circular MP02/2025, 20 November 2025.

74. Working Group 1 - Timely Deployment and Repair, Recommendation (1), 'Streamline Permitting, Approval and Regulation', International Advisory Body on Submarine Cable Resilience, February 2026.

75. Communication with industry rep. 17 December 2025. See also ICPC's bi-annual 'Updates on Submarine Cable Protection and the Environment', which covers issues from volcanic eruptions and turbidity currents to unintended consequences of human activity.

76. A. Palmer-Felgate, 'Global Cable Repair Data Analysis', April 2025; Constable *et al*, 'The Future of Submarine Cable Maintenance: Trends, Challenges, and Strategies, June 2025.

77. 'Security and Resilience of EU Submarine Cable Infrastructures - Mapping, risk assessments, stress tests', October 2025.

78. National Risk Register 2025, https://www.gov.uk/government/publications/national-risk-register-2025

79. For an overview of such measures, see the security and resilience framework proposed in Kavanagh et al, 'Achieving Depth', as well as the series of Strategic and Technical and Support Measures recommended in the EU Cable Security Toolbox

80. Deploying Strategic Cyber Capabilities Across Europe (DIGITAL-ECCC-2025-DEPLOY-CYBER-09), Digital Europe Programme, February 2026.

81. Submarine Cable Repair Capacities-Pilot Works (CEF-DIG-2026-CABLE-REPAIR-CAPACITIES-PILOT), Connecting Europe Facility, February 2026.

82. See, for example, T.Geraghty, 'Managing retention and exit of personnel is key to resolving Defence Forces staffing issue', *Irish Examiner,* 18 February, 2026.

The Institute of International and European Affairs (IIEA) is Ireland's leading international affairs think tank. Founded in 1991, its mission is to foster and shape political, policy and public discourse, in order to broaden awareness of international and European issues in Ireland and contribute to more informed strategic decisions by political, business and civil society leaders.

The IIEA acts as a forum for informed debate, analysis and discussion. Views expressed in the Institute's publications, and in presentations at its events, are those of the authors alone and do not represent the views of the Institute, which is fully independent. The IIEA is a not-for profit organisation with charitable status.

IIEA
Sharing Ideas
Shaping Policy

The Institute of International and European Affairs,

8 North Great Georges Street, Dublin 1, Ireland

T: +353-1-8746756 F: +353-1-8786880

E: reception@iiea.com W: www. iiea.com