Under the Radar: Ireland, Maritime Security Capacity, and the Governance of Subsea Infrastructure

McCabe, R & Flynn, B

Original citation:
McCabe, R & Flynn, B 2023, 'Under the Radar: Ireland, Maritime Security Capacity, and the Governance of Subsea Infrastructure', European Security, vol. (In-Press), pp. (In-Press).
https://dx.doi.org/10.1080/09662839.2023.2248001

DOI 10.1080/09662839.2023.2248001
ISSN 0966-2839
ESSN 1746-1545

Publisher:
Taylor and Francis

European Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/feus20

Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure

Robert McCabe & Brendan Flynn

To cite this article: Robert McCabe & Brendan Flynn (2023): Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure, European Security, DOI: 10.1080/09662839.2023.2248001

To link to this article: https://doi.org/10.1080/09662839.2023.2248001

Published online: 26 Aug 2023.

EUROPEAN SECURITY
https://doi.org/10.1080/09662839.2023.2248001

Routledge
Taylor & Francis Group

Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure

Robert McCabe[a] and Brendan Flynn[b]

[a]Institute for Peace and Security, Coventry University, Coventry, UK; [b]Political Science & Sociology, University of Galway, Galway, Ireland

ABSTRACT

Subsea infrastructure is typically out of sight, but in recent times, seldom out of mind. The sabotage of the Nord Stream pipelines in October 2022 has magnified the vulnerability and critical importance of subsea infrastructure. It also exposed a lack of understanding on how subsea networks operate, how they are regulated, who controls them and how they are protected. Ireland matters in this context. Despite its official policy of neutrality, Ireland occupies an important strategic position in terms of transatlantic telecommunications cables between the United States, Britain and continental Europe. The conflict in Ukraine has amplified tensions in this context in terms of the increased threat of grey-zone/hybrid warfare activity. This article will consider for the first time how a global connectivity hub on the western periphery of Europe governs critical underwater infrastructure. It will discuss the context and agencies involved in subsea cable governance in Ireland and identify the gaps in this protection before formulating suggestions for the long-term improvement of Ireland's maritime security capacity. The Irish case is important as it can help inform defence policy and security practice in other island states with large maritime jurisdictions and in particular states with small navies.

ARTICLE HISTORY
Received 20 April 2023
Accepted 11 August 2023

KEYWORDS
Ireland; Subsea infrastructure; maritime security; Europe; capacity building; Ukraine-Russia

1. Introduction

The apparent sabotage of the Nord Stream pipelines in October 2022 – key subsea pipelines in the Baltic Sea transporting gas from Russia to Europe – has magnified the vulnerability of critical subsea maritime infrastructure.[1] Notwithstanding who is responsible for this act of aggression or why – a topic much speculated on but unresolved at the time of writing – the event has led to discussion in Ireland and further afield in Europe on the ability of states to protect subsurface infrastructure within their maritime jurisdiction and debate around Ireland's capacity to meet its broader maritime security responsibilities (see for example Gallagher 2022, Kenny 2022, O'Keefe 2022). The Nord Stream 2

CONTACT Robert McCabe robert.mccabe@coventry.ac.uk

incident has also exposed a wider lack of understanding globally among policy makers and the public about how subsea networks operate, how they are regulated, who controls them and how they are protected (Bueger and Liebetrau 2021).

In Ireland, maritime security remains an under-prioritised and poorly understood area for policy makers, reflected in a long history of underinvestment in the Irish Naval Service (INS) and in the maritime security capacity of the state. This is not just a problem for Ireland. Traditionally, most European states have opted for more limited policy engagement and less robust governance approaches in relation to the security of subsea infrastructure. This was partly due to an ambiguous international legal regime but also the perceived low threat level (Bueger and Liebetrau 2023, p. 1). Essentially, it was politically easier and more economically viable to outsource responsibility to the private sector to manage and maintain subsea infrastructure regardless of the level of national maritime security capacity or defence partnerships. As Bueger and Liebetrau (2021, p. 405) highlighted in a recent major academic article on cable protection, "so far the global submarine cable network has only been studied in narrow technical terms". They call for recognition of the "increased significance of the network" particularly within debates on maritime security, governance, state building and geopolitics (Bueger and Liebetrau 2021, p. 405). This is complicated further by the inherent complexity of maritime security, where challenges such as subsea infrastructure protection, cannot be comprehensively addressed by any single governance tool or one-size fits all solution (Jentoft and Chuenpagdee 2009). The existing literature tends to focus on historical developments (Hayes 2008, Carter 2009, Mueller 2016); and within this legal, policy and jurisdictional governance (Davenport 2015a, Burnett *et al.* 2019, Guilfoyle *et al.* 2022); scientific and engineering approaches (Xiang *et al.* 2016, Dinmohammadi *et al.* 2019, Ho *et al.* 2020); and more recently, in the field of security studies, in terms of cyber security, critical infrastructure protection, or hybrid warfare (Aradau 2010, Schaub Jr. *et al.* 2017, Trump *et al.* 2020, Bueger and Liebetrau 2023). Hence, there has been limited scholarly engagement around Irish and European maritime security capacity and how it is governed, and far less so, in relation to subsurface security.

Maritime security governance is complex and multilayered. It typically involves multiple stakeholders, crossing multiple jurisdictions and involving the work of multiple agencies (Jentoft and Chuenpagdee 2009, Rode 2017, Flynn and Ó hUiginn 2019, Bueger at al. 2020).

Moreover, as the Irish case reveals, the maritime security space historically lacks the level of public prominence or established practices that security governance architectures ashore can draw upon. This is often termed by scholars as "seablindness" or a socio-political failure to recognise the importance of the maritime domain for the physical and economic security of nations (Mugridge 2009, Germond-Duret and Germond 2022). This picture is further complicated by siloed, hierarchical and overly bureaucratic approaches to maritime security governance in Ireland and elsewhere, which makes it more challenging to reach consensus on how best to respond to security issues in a maritime context (Bueger *et al.* 2020).

Defining maritime security governance is therefore a difficult task. The term maritime security itself is a "buzzword" with no universally agreed definition (Bueger 2015, p. 163). Similarly, different actors understand Critical Maritime Infrastructure in

different ways ranging from a broad focus that encapsulates the protection of all infrastructure with a maritime element (such as ports), to a more technically narrow definition that focuses on a small number of select critical infrastructures (such as subsea data cables) where any level of disruption would create system wide failures. For the purposes of this article, we understand maritime security governance as an umbrella term for the various policy, legislative and operational approaches designed to manage and maintain a secure maritime domain including planning, regulation, deterrence and enforcement.

This article responds to these gaps in scholarly and policy understanding by analysing how Ireland as a global connectivity hub on the western periphery of Europe governs and safeguards its critical underwater infrastructure. It will, for the first time, map the agencies involved in maintaining and protecting subsea infrastructure in Ireland's maritime jurisdiction, critically analyse their respective capacities and establish how they cooperate and collaborate in practice. We then argue that gaps exist in this protection in terms of governance, maritime security capacity and crisis management response. Next, we identify these gaps and provide practical and policy recommendations based on this analysis for how capacity can be improved in the context of preparedness and future threats. This goes beyond monitoring subsea cables, to the development of a more sustainable, equipped and agile Naval Service and marine sector that can meet the complex maritime security tasks of the future in the context of increasing grey-zone/hybrid warfare activity.[2] Recommendations focus on investment in smart technologies and capacity building, updating legislation, increased public/private cooperation, the creation of a single agency with responsibility for maritime security within the state, developing a National Maritime Security Strategy[3] and increased multilateralism.

This analysis will help inform defence policy and security practice in Ireland by mapping out gaps and vulnerabilities, but also provides actionable policy recommendations. In addition, this article will help inform capacity building and resilience measures in other island states with large maritime jurisdictions and in particular states with small navies. This is important, as discourses on security sector reform and state building have not generally integrated subsea infrastructure as core regulatory, security or development challenges (Bueger and Liebetrau 2021, p. 402). Methodologically, this article primarily uses open sources such as government reports and Oireachtas debates, Irish Defence Forces policy documents, academic analysis, alongside industry communications with government and commercial submissions to gain a more holistic insight into the practice and relations between different agencies and bodies.

2. "Gateway to Europe"

Ireland occupies an important strategic position in terms of transatlantic telecommunications cables between the United States, Britain and continental Europe. This enables it to act as a global hub for data centres, which are recognised as core digital infrastructure playing an indispensable role in Irish economy and society (Government of Ireland 2022a). Around three-quarters of all cables in the northern hemisphere pass through or near Irish waters, predominantly off the south coast with

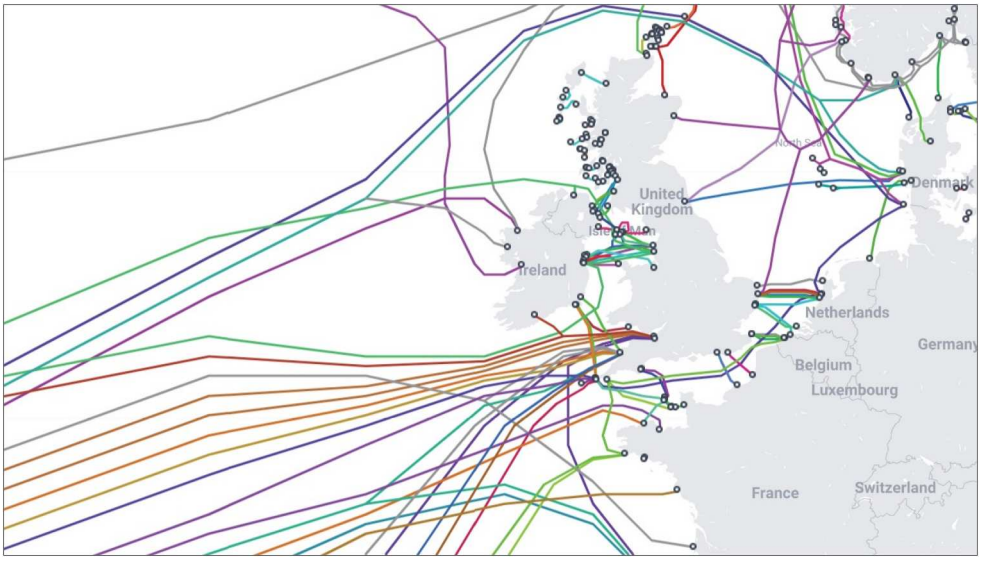

Figure 1. Map of subsea infrastructure in Ireland's maritime jurisdiction. Source: TeleGeography, https://www.submarinecablemap.com.

additional connections off the northwest coast (see Figure 1). This spatial concentration reveals how small states like Ireland can be pivotal for the wider security of allied and friendly neighbouring states. However, given the inherent resource and capacity restraints of smaller states, they may also serve as a weak link in that security assemblage.

These transatlantic cables carry a large percentage of global communications, including financial transactions, business operations and everyday internet access (O'Keefe 2022). At the time of writing, four of these transatlantic cables physically connect to Ireland, with a further 12 connecting Ireland and Britain. As technology develops, submarine fibre optic cables are now also extensively relied upon by militaries, the oil and gas industry, as well as the scientific community (Davenport 2015b, p. 58).

Ireland's energy security is also heavily reliant on subsea infrastructure. For example, around 75% of Ireland's gas demand is met by two subsea interconnectors from Scotland (Department of the Environment, Climate, and Communications (DECC) 2022, p. 16). Electricity interconnectors also link Ireland to the UK and, by 2027, also with France (DECC 2022, p. 16). In November 2022, a new subsea cable was opened connecting Ireland to Iceland. This was the first time an underwater cable had been connected to Ireland that was not linked to Britain or North America with planning underway for two additional cables to connect Ireland with Japan and later Portugal (Killeen 2022).

In response to the sabotage of the Nord Stream pipelines, former Irish Minister for Defence Simon Coveney announced that Ireland was to intensify security around its offshore infrastructure (Houses of the Oireachtas 2022a). This included increased patrols by the INS and Air Corps and targeted surveillance of subsea data cables. While this was a positive recognition of the importance of this infrastructure, it did not solve the issue that the State's principal sea-going agency – the INS – does not currently

have the required subsurface capabilities or enough assets at sea at any one time to effectively undertake the broader maritime security responsibilities of the state. The INS's current vessels are austere and lack NATO standard sonars capable of detecting, classifying and tracking either submarines or submersibles.

Other countries have taken a more proactive approach in terms of subsea defence in the wake of the Nord Stream incident. The UK government, for example, announced the commission of two new undersea surveillance ships due to be operational by Summer 2023 (Gallagher 2022, UK Ministry of Defence 2023). Sweden, was also notably able to quickly dispatch a vessel capable of advanced diving missions to the Baltic Sea area to assess the ruptured undersea pipelines (Olsen 2022). At the EU level, a fifth wave of Permanent Structured Cooperation (PESCO) projects were announced in May 2023. This included a dedicated project led by Italy on subsea critical infrastructure, although at the time of writing, Ireland has not yet decided to join this specific project (see PESCO 2023). One obvious problem for any EU led framework will be how to integrate with the relevant UK authorities, particularly in the context of Brexit-related institutional complications. Given the spatial distribution of subsea cables, a high degree of cooperation between the UK, Republic of Ireland and the EU should be essential.

Ireland's ongoing support for promoting subsea cable development links to a broader Irish Government strategy of establishing Ireland as a "gateway to Europe" in terms of telecommunication connectivity (Killeen 2022). While investment in more subsea cables increases resilience in the form of redundancy, it also brings with it extra vulnerability from intentional acts of sabotage or criminal interference. Redundancy here refers to the existence of multiple cables between two nodes, which means data transmission may take multiple paths, in the case where one cable is damaged for example (Brodsky 2018). According to Cottey (2022, p. 4), "the highly globalised nature of the Irish economy and the presence of major multinational companies and significant internet server farms make the country a particularly attractive target for cyber-attacks, whether by criminal groups, 'rogue states' or major powers". A somewhat separate threat is the relatively undetermined potential for non-destructive but possibly damaging "parasitic" signals intelligence operations by state, or possibly non-state, actors who could target subsea cables for "tapping". A precedent exists for this in that during the Cold War there were some documented cases of intelligence "tapping" of submarine telecommunications (Craven 2001). However, industry experts suggest that cyberattacks, such as hacking, phishing, or whaling, are much more likely to occur than physical intervention at sea (Hillman 2021, p. 2). Not only do they have a greater chance of success, cyberattacks avoid the added complexity of operating underwater. In addition, it is highly unlikely that a submarine cable can be tapped without immediate detection (European Subsea Cables Association 2023).

The Nord Stream incident highlighted how intentional acts against subsea infrastructure can also be dramatically kinetic in nature, exposing the inherent vulnerabilities of infrastructure under the sea. This coupled with Ireland's limited maritime security enforcement capacity, in particular a notable lack of subsurface capabilities, means that subsea infrastructure traversing Ireland's maritime jurisdiction is particularly exposed to these potential threats. This has led to contentions that Ireland is a "weak link" in terms of European security and defence (Drea 2022, McNamara 2022, Mooney 2022).

While documented intentional acts of criminal damage or grey-zone sabotage against subsea infrastructure are rare, the potential impact of a large-scale disruption is substantial. Therefore, contingency planning and capacity building to monitor, detect and deter hostile acts against such infrastructure is critically important for states such as Ireland. Apart from the physical and economic damage arising from a large-scale disruption, the reputational damage to Ireland as a "gateway to Europe" would likely be profound with potential negative impact on foreign direct investment, which accounted for 28% of the State's nominal GDP in 2022 (CEIC Data 2023).

Although rare, intentional acts against subsea cables have been documented. In 2007, for example, two active submarine cable systems were extensively damaged by Vietnamese fishing vessels in an attempt to recover copper components. The International Cable Protection Committee (ICPC) (2009) described these actions as "acts of piracy" under the United Nations Convention the Law of the Sea (UNCLOS). In 2013, three divers allegedly attempted to cut the SEA-ME-WE 4 cable off the port of Alexandria during the Egyptian Crisis (Kazaz 2022, p. 54-57). More recently, in March 2023, Taiwan accused Chinese ships of cutting subsea cables between the mainland and one of the outlying islands (Wu 2023). The ICPC has described the threat from these types of activities as "unprecedented" in the history of submarine cables and that the threat has the capacity to cause "tremendous disruption to the telecommunications network" (ICPC 2009). However, it should be noted that the vast majority of damage to subsea cables is caused by fishing vessels or ship's anchors rather than malicious acts. For example, in October 2022, the SHEFA-2 communications link between the Faroe Islands, Shetland and Scotland was severed. Initial speculation was that it may have been an intentional act of sabotage, but it later transpired it was inadvertently caused by a fishing vessel (Martin 2022).

Apart from the threat from criminally motivated acts, the apparent sabotage of the Nord Stream pipelines highlights the vulnerability of subsea infrastructure in the context of increasing hybrid or grey-zone activity. The conflict in Ukraine has amplified tensions in this context with reports from An Garda Síochána (The Irish Police) and Defence Force sources that Russia had sent intelligence agents to Ireland to map the precise location of fibre-optic subsea cables in 2020 (Ankel 2020, Mooney 2020, The Moscow Times 2020). In 2021, it was also reported that the Russian vessel *Yantar* deployed an AS-37 mini-submarine, which was able to submerge to a depth of 6000 m off the Irish coast, following the route of Norse and AEConnect-1 cables, which link Europe to the United States (David 2022).

2.1. (Sub)seablindness

Despite their strategic importance, the security of subsea cables is an understudied element of Irish and European security policy, only recently pushed into the limelight following the Nord Stream incident. Therefore, it is not surprising that Ireland, like many other European countries, has not afforded any real strategic priority to their protection. This links to what Bueger and Liebetrau describe as the "triple invisibility" of subsea infrastructure (Bueger and Liebetrau 2021, p. 392). Firstly, that core infrastructure tends to be taken for granted and therefore overlooked; secondly, that since cables exist under the surface they are among the least visible type of physical infrastructure; and thirdly, since submarine data cables are not only under the surface, but also at sea, their

invisibility is further intensified. Despite this, and as outlined in a submission to the Commission on the Defence forces in 2021 (Speller 2021, p. 2), "Irish guardianship over a huge maritime space, within which critical trade routes pass and under which key trans-Atlantic internet cables are positioned, gives us responsibilities that cannot be ignored, and that require us to adjust previous practice and policies".

Subsea infrastructural security (alongside broader maritime security) is an area that has largely been neglected by policymakers in Ireland. For example, the updated Irish White Paper on Defence of 2019 only mentions subsea cables once – "Ireland's energy security is therefore heavily reliant on a relatively small number of vital installations, both onshore and sub-sea" – with no provision for how they might be protected from intentional acts of sabotage or aggression (Government of Ireland 2019a, p. 34). Similarly, there is no mention of subsea cables in the National Cyber Security Strategy (2019–2024), despite the emphasis on the protection of internet connectivity and data integrity from deliberate actions by organised groups, including Nation States, seeking to subvert or compromise these systems (Government of Ireland 2019b, p. 3). Despite their obvious prominence in this context, subsea cables are not explicitly identified as "critical national infrastructure" in Ireland, in the same way that offshore wind turbines might be considered for example. This is despite meeting the criteria to rank at the highest level on the "criticality scale" as outlined in the Irish Government's Strategic Emergency Management report (Government of Ireland 2020, p. 15).

The Department of the Environment, Climate, and Communications launched a public consultation process on international connectivity for telecommunications in October 2020 to inform policy development and decision-making (DECC 2020). The key findings of this consultation process make no mention of how to protect or secure cables from sabotage or intentional acts of degradation. Most risks relate to corporate and governance concerns including the impacts of Brexit. The only physical risks identified are natural ageing of the cables or damage from fishing vessels or ferries (DECC 2021). However, a closer examination of the consultation submissions reveals that there are security concerns within industry. Aqua Comms, in the most comprehensive submission, outlined several specific security concerns notably on the absence of guidance on how submarine cables would be protected in the event of increased risk (Aqua Comms 2020, p. 6). They also raise concern that the current planning and marine licence application process requires publication of detailed plans including the location of cable landing stations, route maps, and associated documentation, which could be exploited by terrorist groups or state actors wishing to disrupt global telecommunications (Aqua Comms 2020, p. 7).

3. Legislation governing subsea infrastructure in Ireland

Ireland's unique geographical positon has facilitated its development as a hub for transnational telecommunications since the mid-nineteenth century. The first transatlantic cable was laid between Newfoundland and Valentia Island, Co. Kerry, in 1858, facilitating a new era of transatlantic communications (Whittaker 2020). The first appearance of legislation in Ireland (then as part of the UK) for the protection of subsea cables came in 1884 with the ratification of the Convention for the Protection of Submarine Telegraph Cables. The Act recognised the threat to nascent subsea cables from "wilful"

(e.g. intentional acts of sabotage) or "culpable negligence" (e.g. damage from fishing related activities) (Submarine Telegraph Act 1885). The Foreshore Act of 1933 also pertains to subsea governance in terms of licensing for landing sites; arguably, the most vulnerable point of submarine cables and remains a key piece of legislation in this regard (David 2022).

The primary international legislation that establishes the legal responsibilities of states in relation to subsea infrastructure in Ireland and elsewhere is the Geneva Conventions on the Continental Shelf and the High Seas of 1958 and the UNCLOS adopted in 1982. Article 21 of UNCLOS outlines that states may adopt laws and regulations in the territorial sea for the protection of subsea cables and pipelines (UNCLOS 1982, p. 31). Article 79 covers the rights of states with regard to submarine cables and pipelines on the continental shelf primarily in terms of laying, maintenance and repair. Most significant is Article 13 that requires states to enact legislation to punish offenders who interrupt or obstruct telegraphic or telephonic communications wilfully or through culpable negligence (UNCLOS 1982, p. 64). Essentially, all states and their nationals have the legal right to lay and repair cables outside of any state's territorial waters. Unlike ships, subsea cables do not come under the flag of any single state and, therefore, legal ownership is divided among various co-owners, resulting in a "legal kaleidoscope of jurisdictions and nationalities" (Burnett 2021, p. 1668). This also means that there is no statutory government requirement to restore traffic if a cable is damaged or disrupted (Burnett 2021, p. 1665).

Despite the requirements outlined under Article 13 of UNCLOS, many states have not created the requisite domestic legislation to prosecute for specific acts of aggression against subsea infrastructure. As Davenport (2015a, p. 106) highlights, Article 113 may not be particularly useful, considering that many States have not implemented their obligation to adopt national legislation. Ireland is no exception. The Maritime Security Act of 2004, for example, makes no explicit reference to the protection of subsea cables or pipelines. However, the act does empower the INS, when acting at the request of An Garda Síochána, to counter unlawful acts against the safety of maritime navigation, subsea telecommunications cables and fixed platforms within the area of the continental shelf (Maritime Security Act 2004, Government of Ireland 2022b).

The Maritime Area Planning Act 2021 is one component of the National Marine Planning Framework (NMPF). One of the aims of NMPF is to streamline the provision of subsea fibre optic cables to provide international telecommunications capacity into the future (Government of Ireland 2022c, p. 95). The Maritime Area Planning Act itself outlines the conditions for the protection of underwater cables, wires, pipelines that a coastal planning authority may attach to development permission in the nearshore area (Maritime Area Planning Act 2021, p. 156). A newly created body – the Maritime Area Regulatory Authority (MARA) – will enforce these legislative acts. Apart from its compliance and enforcement role, MARA will also support delivery of projects of strategic importance including cabling and telecoms projects when it becomes operational in 2023 (Maritime Area Regulatory Authority 2023). Alongside these legislative and regulatory instruments, there are abroad range of government departments and agencies with responsibilities in the maritime domain (see Table 1).

Table 1. Irish governmental departments and agencies with responsibilities in the maritime domain (Government of Ireland (April 2022) Department of Defence Capability Review, p. 30. https://assets.gov.ie/230958/8a470703-3e0b-4397-b80c-cbb3cc48ea12.pdf).

Entity	Roles
Department of Transport	National maritime safety and port security.
Department of Agriculture, Food and the Marine	Security of maritime resources, especially in promoting compliance with the EU Common Fisheries Policy and sea fisheries law.
Sea Fisheries Protection Authority	
Department of the Environment, Climate, and Communications	Cyber security and pollution at sea.
Department of Justice	Maritime Security Act (2004) empowers the Irish Naval Service, when acting at the request of An Garda Síochána, to counter unlawful acts against the safety of maritime navigation, sub-sea telecommunications cables and fixed platforms within the area of the continental shelf.
Office of the Revenue Commissioners	Combat the smuggling of illicit narcotics and other contraband.
Commissioners of Irish Lights	Aids to navigation, search and rescue, maritime consultancy.

The operators of subsea telecommunications cables are also subject to the provisions of the Authorisation Regulations (SI 335 of 2011) and are bound by the conditions of their General Authorisation, which includes the condition to take all measures necessary to ensure the security of public electronic communications networks against unauthorised access (Houses of the Oireachtas 2021b).

4. Gaps in Ireland's protection and governance of subsea infrastructure

4.1. Governance

It is clear there are gaps in how Ireland governs and secures subsea infrastructure (and maritime security more generally). Central here is the lack of a single agency with responsibility and oversight of such matters. According to Burnett *et al.* (2019, p. 9), "because States do not appear to have anticipated or appreciated the critical nature of submarine cables to their international communications, there is often no lead agency to coordinate effective policies on submarine cables".

Currently, there are at least five separate government departments operating alongside multiple state agencies and private sector companies with different responsibilities for the governance and security of subsea infrastructure (see Table 1). Relationships between these entities are managed by a variety of means, most notably through Service Level Agreements. This overly bureaucratic approach to maritime governance has led to policy silos, which can ultimately result in fragmented policy decisions where there is limited inter-departmental cooperation, engagement with the private sector, or cross-fertilisation of ideas (Flynn and O'hUiginn 2019, p. 8, Burnett *et al.* 2019, p. 9). This is reflected in the 2020 consultation process on international connectivity for telecommunications, where it was suggested that a forum was needed for submarine cable operators to provide feedback to government on major challenges, barriers or recommendations to improve or innovate within the sector (DECC 2021, pp. 19–22). It further reflects the "fragmented state" of maritime security governance in Ireland more broadly, which as the Department of Defence's Capability Review outlined, is epitomised by the fact that the Marine Attaché post in Brussels is co-funded by five separate government departments (Government of Ireland 2022b, p. 31).

Apart from this messy governance picture, at the operational level, the INS – the state's primary agent for maritime security – are not formal consultees in the foreshore licensing process for subsea cables. This means that they would not automatically have access to the location of new cables for example, which is an obvious shortcoming. In addition, there are no special permission requirements to apply for the foreshore license to survey and install subsea cables in Irish waters – this differs from most other countries that require an operator's licence (permission from the state). In the United States, for example, prospective cable operators require a Federal Communications Commission licence. This links to the fact that subsea infrastructure is not considered critical national infrastructure in Ireland, which is a significant gap in how subsea infrastructure is prioritised in term of security governance.

Finally, Ireland's lack of a National Maritime Security Strategy (NMSS) is a noteworthy policy gap. This is because a national strategy can act as an important governance tool to provide overall direction and continuity in maritime security policy among the different government departments and the various public and private sector agencies operating in the state (SafeSeas 2018, p. vii). At the time of writing, a NMSS is being considered in the context of developing the National Security Strategy (Government of Ireland 2022b, p. 31).

4.2. Maritime security capacity

For Ireland, maritime security is an important, multi-faceted and complex area of national policy (Government of Ireland 2022b, p. 30-31). Despite this, it remains a poorly understood area for policy makers, reflected in a long history of underinvestment in the maritime security capacity of the State. This enduring "seablindness" is perhaps the most fundamental gap in Ireland's ability to monitor, disrupt or deter intentional acts against subsea infrastructure within its maritime jurisdiction.

Historically, there are multiple reasons for underinvestment in Irish maritime security and defence, notably, an apparent lack of existential threats to the state combined with its post-colonial legacy and geographical position. This means that Ireland has traditionally, and largely unofficially, relied on its neighbour Britain to undertake the "heavy lifting" in terms of defence. For example, in March 2020, RAF Typhoon jets were scrambled twice to monitor Russian bombers that had entered Irish-controlled airspace off the western coast (Murphy 2022). According to an article in the UK Defence Journal, "In short and simple terms, the UK is protecting its own airspace and Ireland benefits from that" (Allison 2022). Gaps in maritime security capacity also link to sensitives around the idea of neutrality or military non-alignment. In this respect, it can be argued that Ireland partially exhibits behaviour that is closer to the defence and security practices of microstates (Wivel and Oest 2010). This implies a reliance on ad-hoc and implicit outsourcing of external security to neighbouring powers rather than classic small state strategy, which typically favours membership of defence alliances (e.g. NATO) or, alternatively, a strategy to resource an autonomous defence stance. There are signs of a shift here however. At the time of writing, the Irish Government, through membership of the NATO-led Partnership for Peace (PfP), is giving "deep consideration" to participating in NATO's Critical Undersea Infrastructure Coordination Cell as well as relevant EU PESCO projects (Leahy 2023, Phelan 2023). The

Critical Undersea Infrastructure Coordination Cell will facilitate engagement with industry and bring key military and civilian stakeholders together to share best practices, leverage innovate technologies, and boost the security of undersea infrastructure (NATO 2023). Crucially, because it is a NATO initiative, the UK is by default a major player whereas Ireland only has a basic partnership agreement with the alliance. This illustrates how overlapping EU and NATO memberships are becoming important but also problematic.

Other neutral European nations have invested heavily in maritime security capacity in comparison to Ireland. Sweden, for example, a neutral state until only very recently, possesses a naval flotilla capable of conducting military operations, intelligence gathering, and surveillance on, above and under water (Swedish Armed Forces 2023). A report by RUSI highlighted that "without collective defence guarantees, Ireland's cyber, airspace and naval defences remain underdeveloped and are inadequate for a neutral state that can, in theory, only rely on its independent military capacity" (McNamara 2022a).

At the time of writing, the INS has a flotilla of eight ships including offshore and coastal patrol vessels (Irish Defence Forces 2023a). Two new ships purchased from New Zealand will not be operational until 2024 at the earliest (Irish Department of Defence 2023). However, crew numbers have dropped by 25% since 1998, and at times only half the ships are active at sea at any one time chiefly due to staffing and maintenance issues (O'Keefe 2021). The last time all ships were in service in a single year was in 2018 with a measurable impact due to Covid-19 (Gallagher 2021). Currently, these vessels lack advanced capacity to detect activity in the air or below the surface. They are not, according to Ian Speller (2021, p. 2), "the three-dimensional assets that one would find in the navies of other European states of comparable size and wealth".

The INS does have capabilities beyond Automatic Identification System (AIS) tracking. This includes satellite tracking, which enables awareness of what types of vessels are operating in Irish waters and the ability to identify and contact vessels for further clarification. However, significant gaps remain in that the service does not possess any advanced underwater surveillance equipment such as NATO standard sonars capable of detecting, classifying and tracking either submarines or submersibles (Murphy 2022, Irish Defence Forces 2023a). As John Brady TD commented, "Due to our limitations, first in terms of personnel but also in terms of subsurface surveillance, our ability to monitor what is happening to [subsea] cables is highly limited, putting our security and the European project at risk" (Houses of the Oireachtas 2021a).

More recently there are signs of the government's increasing commitment to support the transformation of the Defence Forces into a more modern and agile force, capable of responding to increasingly complex security threats. Following recommendations set out Report of the Commission on the Defence Forces, for example, the government made the decision to purchase a primary surveillance radar system, a capability that Ireland did not previously possess (Irish Department of Defence 2022, p. 17). In addition, a tender was issued for a Multi Beam Echo Sounder kit for up to four vessels in mid-2022, which, when it materialises as a working capability, will give the INS a basic ability to map and monitor sea bed activity (Office of Government Procurement 2022).

4.3. Crisis management response

As discussed, in the event of an intentional attack on subsea infrastructure, Ireland lacks the capacity to launch an effective response that might extend to pursuing and apprehending an offender. In practice, the private sector finances, constructs, owns, operates, maintains and repairs subsea and other offshore infrastructure often through third-party private operators with much of the interaction between state agencies (such as the INS) carried out on an ad-hoc basis. This expertise, including knowledge of the state of the art in terms of technological advancements, is only available to a limited degree among governmental agencies, and therefore closer collaboration between all actors is critical (Bueger and Liebetrau 2023, p. 5). In the event of an intentional act of sabotage or aggression against a telecommunication cable, for example, the privately owned and operated Network Operating Centre (NOC) would be immediately alerted.[4] The telecoms operator would then contact the Atlantic Cable Management Association (ACMA) in the first instance, which have a limited number of vessels available 24/7 to repair cables. The NOC will examine AIS information to determine the potential cause of the disruption such as a suspicious vessel in the area. If a ship turns off its AIS, however, it would be undetectable. In this context, interaction with the state would be beneficial but such interaction does not take place at present at least in a formal way.

In terms of the state's role, location is the first thing to consider. If an attack occurs within territorial waters (12 nautical miles (nm) from the coast) the company's point of contact would be An Garda Síochána – a force with a limited maritime component via the water unit. Beyond 12 nm, the cable operator would contact the Irish Coast Guard in the first instance as the designated lead state agency operating in this context under the oversight of the Department of Environment, Climate Change and Communications. However, the Coast Guard has no mandated security role and is primarily a maritime search and rescue agency with limited offshore boats or helicopter capabilities (Irish Department of Transport 2022). The INS is not the lead agency with responsibility for monitoring and responding to security events related to subsea infrastructure despite its broad maritime security remit. However, in practice, the navy does frequently fulfil this role, for example, in the case of the *Yantar*, the navy reportedly identified and monitored the ships activity.

The INS does currently have a limited capacity to undertake such tasks via the Fisheries Management Centre, which carries out monitoring and surveillance of all vessels equipped with a Vessel Monitoring System (VMS) operating in the Irish Exclusive Economic Zone (EEZ) (Irish Defence Forces 2023b). The Fishery Protection System known as "Lirguard" has relevant systems here, such as the Fishery Information System (an application used to capture, maintain and report on information regarding vessels), and the Fishery Geographic System (enables a range of spatial and analysis operations). The INS have increasingly evolved a Recognised Maritime Picture (RMP) of the Irish EEZ which combines a fusion of data points from AIS, VMS and radio traffic and intelligence analysis, as well as incidental or planned Air Corps observation reports and radar tracks. Yet this RMP is currently limited to surface contacts and is not as advanced or as systematic as equivalent RMPs generated by NATO member states of the EU.

5. Increasing preparedness: recommendations to meet future threats

Figure 2. Authors.

5.1. Increased investment in smart technologies and maritime security capacity

Ireland's limited maritime capacity alongside the current staff retention and budgetary issues in the INS, suggest that more innovative and smart technology solutions, such as the use of autonomous systems and uncrewed vessels, should be considered. In comparison to larger investments, such as patrol vessels, autonomous systems tend to be cheaper, more durable and maintain a lower profile and can improve Ireland's capacity to respond to and deter threats across the full spectrum of the maritime security space (Dunley 2023, p. 5). We suggest this should focus on three areas: (1) Unmanned Undersea Vehicles (UUVs), such as the Kongsberg Seaglider, which can offer more "tactical flexibility" and complement Distributed Acoustic Sensing technology used by the private sector for detecting subsea cable faults in real time (EU Commission 2022, Mugg *et al.* 2016, p. 21). (2) Remotely Piloted Air Systems (RPAS) and Unmanned Aerial Vehicles (UAV) including artificial intelligence equipped drones to increase Maritime Domain Awareness. (3) A shipborne towed sonar array to complement the Air

Corp's 2023 purchase of two CASA C-295 maritime patrol aircraft, which while capable, lack advanced sonar and sonobuoy equipment (Houses of the Oireachtas 2022b). Meeting the accepted recommendations set out in the Report of the Commission on the Defence Forces will go some way to bolstering Ireland's maritime security capacity in this regard. Notably the development of a primary radar capability, anti-drone and counter Uncrewed Aircraft System capabilities, and the further development of RPAS capabilities (Irish Department of Defence 2022, p. 29). However, implementing these recommendations requires the requisite political will, social capital and long-term investment but they would contribute to the creation of a more level playing field while also acting as a force multiplier (Figure 2).

5.2. Legislative update

Ireland, like many other European counties, lacks contemporary legislation that reflects the critical importance of subsea infrastructure security and governance. In this regard, subsea infrastructure should be recognised as critical national infrastructure by the State as a primer for the development of "international co-operation between States in devising and adopting effective and practical measures for the prevention of all unlawful acts against the safety of maritime navigation" (Maritime Security Act 2004, p. 10). Practical measures might include increasing penalties for interference with subsea infrastructure or extending international law to protect cable systems and operator vessels from hostile acts (ICPC 2009). In this regard, legislation could be adopted that designates the INS as the lead state co-operative agency with responsibility for monitoring and protecting subsea infrastructure and not the Coast Guard or An Garda Síochána. This is because the INS is the only Irish state agency with a proven and credible sea-going capability to either deter, detect or intervene and effect state power at sea.

5.3. Closer engagement with the private sector

The vast majority of transoceanic digital communication cables are privately owned and, in the Irish case, privately protected. For example, EirGrid has a private company providing surveillance and monitoring capability for its undersea network via Global Positioning System tracking (Houses of the Oireachtas 2022a). Therefore, closer engagement with the private sector is crucial to secure cables, to set standards for security, and promote those standards globally (Congressional Research Service 2022, p. 20). The lack of a common platform where government and industry can engage on sensitive issues, data and threat information around subsea infrastructure is a significant gap. The ICPC recognises such engagement as best practice and highlights that the sharing of risk and incident data between operators and governments is useful for identifying patterns of activity, gaps in existing cable protection efforts, areas for improving resilience and identification of malicious acts by state and non-state actors (ICPC 2021). In addition, the INS should be consultees in the cable planning and application process and an INS member should be designated as a liaison officer to the subsea industry to facilitate the exchange information and updates as they pertain to security related matters specifically.

5.4. Creation of a single agency

The creation of a single agency within the Department of Defence or Transport for example, with responsibility for maritime security would help tackle the inefficiencies currently experienced by multiple agencies frequently operating in silos. The new Maritime Area Regulatory Authority could be repurposed towards this end potentially. Such an entity could mirror the recently created Joint Maritime Security Centre in the UK, which aims to "increase awareness and understanding of maritime security threats and enable cross-government coordination to deliver a whole-system response to mitigate them" (UK Government 2023). Alternatively the entity could adopt an "information fusion centre" type model (or borrow elements from this model), whereby information on particular maritime security threats are received, analysed, and pertinent information is shared with the relevant authorities (see for example Information Fusion Centre 2023). Here, the existing components of the Fishery Protection System and Lirguard can be utilised. Within this agency, there could be a National Critical Infrastructure Committee to coordinate and manage crisis response in the event of suspicious activities or acts of intentional disruption to subsea infrastructure. This could be supported by an intelligence-gathering element in the context of disrupting and deterring maritime cyber-attacks supported by existing national agencies such as the National Cyber Security Centre. Subsea infrastructure protection would be just one element of the new agency. Other branches would focus on additional maritime security related issues for the state such as fisheries crime.

5.5. Development of a national maritime security strategy

This article proposes two possible approaches for the development of an Irish NMSS. Firstly, Ireland develops an independent national maritime security strategy that aligns closely with the EU Maritime Security Strategy 2014 (EUMSS) but recognises Ireland's unique national governance structures, agencies, challenges and available capacities (see Council of the European Union 2014). Secondly, Ireland forgoes a national strategy and instead contributes to the development and adaptation of the forthcoming updated EUMSS. This is not an exceptional approach, as other EU maritime states, such as Portugal and Denmark, do not have national strategies. However, both these states have much larger and stronger maritime sectors and navies that work within NATO standards, structures and technology levels. The main issue with the second option is the potential lack of buy-in nationally for a country already struggling with maritime security capacity and "seablindness" issues. The advantage of developing a new strategy is the opportunity to engage multiple stakeholders (public, military, industry, etc.) to feed into the process from the start thus leading to a potentially more inclusive, impactful and sustainable strategy – and vitally increasing national awareness of the importance of a secure maritime domain for a state like Ireland. As outlined in a report published by SafeSeas, "it is vital that these are drafted through broad consultative processes and should include a review and accountability mechanism" (SafeSeas 2018, p. vii).

5.6. Increased multilateralism

Closer partnership with other EU Member States or NATO (through the PfP) is an obvious method by which Ireland can enhance its intelligence, situational awareness. and

technological expertise in relation to subsea infrastructure security. This might include joint training, intelligence sharing, technological development, equipment maintenance, or possibly joint procurement and pooling of assets. As Germond and others have pointed out, "today a growing number of so-called small navies possess the capabilities to operate within coalitions, often under the auspices of international organizations" (Germond 2014, p. 40-41). This type of approach can help smaller states expand their maritime portfolio with relatively little risk and allow them to "reasonably compensate for their smallness" (Till 2014, p. 29). As Cottey (2021, p. 12) explains, "cooperation with European partners may be an important way for Ireland to achieve economies of scale while retaining effective military capabilities". This approach is also supported by the ICPC, which recommends that states undertake naval exercises and war games involving the submarine cable industry to test protocols in an international setting (ICPC 2009).

6. Conclusion

Investing in, maintaining and protecting subsea infrastructure is vital to Ireland's national strategic interests as a "gateway to Europe". The ongoing conflict in Ukraine and, in particular, increasing grey-zone hybrid activity such as the Nord Stream pipeline incident, is a reminder that Ireland cannot disregard the increasing complexity and insecurity permeating global geopolitics. Neutrality and military non-alignment do not conflict with judicious investment in maritime security and defence capacity, particularly for an island nation with a maritime jurisdiction some ten-times its landmass (Marine Institute 2022).

This article has attempted to situate Ireland's relationship with subsea infrastructural governance in this broader European and international security context and has highlighted how Ireland, like many other European countries, has not paid adequate attention to how subsea infrastructure is governed and secured despite its critical role as a social and economic conduit. Therefore, while it is always out of sight, it should not be out of mind.

Despite its geographical location and long history as a transatlantic telecommunications hub, there are significant gaps in how Ireland governs and secures the critical subsea infrastructure that traverses its maritime spaces. Firstly, there is an overly bureaucratic and siloed governance arrangement with multiple public and private agencies involved often cooperating in an ad-hoc manner. Secondly, maritime security capacity is underfunded and, when coupled with a Naval Service retention crisis, means that there is limited ability to know what is happening both on and beneath the ocean's surface. Finally, the muddled governance picture means that coordinating a response in the event of a malicious act against a subsea cable or pipeline predominantly falls on the private sector to manage in the first instance.

While steps are being taken at a policy level to build a more capable maritime security capacity, there needs to be more research and investment into understanding the different types of maritime security threats faced by Ireland and how they might manifest in the future. This is particularly prescient as "the dependence between the maritime order and global prosperity is only likely to grow" (Patalano 2023). Traditionally, Ireland has been predominantly reactive in the face of responding to security threats and crises – so there is a need to promote increased preparedness and enhance the states' predicative ability to meet future threats in a more informed and cost effective way. This entails delegating

resources in a more prudent fashion and ensuring the INS has the capacity to meet the maritime security responsibilities of the state. This includes increasing investment in novel technologies alongside maritime security and defence capacity, reviewing and updating existing legislation, working in closer partnership with the private sector, increasing efficiency through the creation of a single point of contact and development of a national strategy for maritime security, as well as increased interoperability with European partners. These recommendations have applicability beyond the Irish case, and can help inform defence policy and security practice in other island states with large maritime jurisdictions and in particular states with smaller navies.

This article has also considered to what extent Ireland is a "weak link" as regards subsea cable security for the wider EU and NATO. Because Ireland is not a NATO member means any, possibly Russian, intelligence or sabotage operation in the Irish EEZ or even territorial waters has lower diplomatic risk. Given the tensions of the Ukraine war and the sabotage by some entity of the Nord Stream 2 pipelines, that scenario is far from fanciful. Indeed the logic of horizontal escalation would make it a plausible and lower risk strategy for raising the stakes with NATO countries by hitting them indirectly via critical infrastructure that passes through a non-NATO state. There is also evident a historic pattern from the Irish state of extensive levels of outsourcing and under-provisioning of external security and defence capability. Other small states, even those who are not NATO members, do not underspend on their military or naval capabilities to the same extent or for so long. The result is a cumulative lack of credible subsea security capability whose implications are possibly stark not least for Ireland but also for the wider EU and NATO. There is evidence of growing awareness among Irish policy elites, but the critical weakness in legal, institutional and technological infrastructure remain including the enduring lack of a National Security Strategy. For these reasons, Ireland faces a significant challenge to address its subsea infrastructure security and in that, provides a heightened level of threat well beyond its maritime borders.

Notes

1. Subsea infrastructure in the context of this article covers both data cables and oil and gas pipelines.
2. Grey-zone/hybrid warfare refers to strategies of aggression that combine covert operations conducted by special-operations forces, sabre-rattling and information warfare as opposed to direct military confrontation (Hughes 2020).
3. Ireland does not currently have a National Security Strategy although one is in development at the time of writing.
4. A Network Operations Center (NOC) is a centralised place from which administrators supervise, monitor and maintain a telecommunications network (Awati 2023).

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Allison, G., 2022. Do British fighter jets 'protect' Irish airspace? No. *UK defence journal*, 19 June.

Ankel, S., 2020. Russian intelligence agents reportedly went to Ireland to inspect undersea cables, and its reigniting fears they could cut them and take entire countries offline. *Business Insider*, 17 February.
Aqua Comms, 2020. Submission on international connectivity for telecommunications consultation, 27 November. Available from: https://assets.gov.ie/138016/876e72e2-ede1-4d6a-9b7f-debfb11f524e.pdf.
Aradau, C., 2010. Security that matters: critical infrastructure and objects of protection. *Security dialogue*, 41 (5), 491–514.
Awati, R. 2023. Network Operations Center. *TechTarget*. Available from: https://www.techtarget.com/searchnetworking/definition/network-operations-center.
Brodsky, P. 2018. Submarine cable redundancy, explained. *TeleGeography*, 2 May. Available from: https://blog.telegeography.com/what-is-submarine-cable-redundancy.
Bueger, C., 2015. What is maritime security? *Marine policy*, 53, 159–164.
Bueger, C., Edmunds, T., and McCabe, R., 2020. Into the sea: capacity-building innovations and the maritime security challenge. *Third world quarterly*, 41 (2), 228–246.
Bueger, C., and Liebetrau, T., 2021. Protecting hidden infrastructure: the security politics of the global submarine data cable network. *Contemporary security policy*, 42 (3), 391–413.
Bueger, C., and Liebetrau, T., 2023. Critical maritime infrastructure protection: what's the trouble? *Marine policy*, 155, 1–8.
Burnett, D.R., 2021. Submarine cable security and international law. *International law studies*, 97, 1659–1682.
Burnett, D.R., Beckman, R., and Davenport, T.M., 2019. *Submarine cables: the handbook of law and policy*. Leiden: Brill.
Carter, L., 2009. *Submarine cables and the oceans: connecting the world*. Cambridge: UNEP-WCMC.
CEIC Data, 2023. Ireland Foreign Direct Investment. Available from: https://www.ceicdata.com/en/indicator/ireland-foreign-direct-investment–of-nominal-gdp.
Congressional Research Service, 2022. *Undersea telecommunication cables: technology overview and issues for congress*, September 13, R47237.
Cottey, A., 2021. Submission to the Commission on the Defence Forces, March. Available from: https://assets.gov.ie/136081/b3253378-6133-467e-a5c0-0dd0addd1ab0.pdf.
Cottey, A., 2022. A Celtic Zeitenwende? Continuity and change in Irish national security policy. *In*: B. Flynn, L. Walshe, S. Quinlan, and S. Molumphy, eds. *Defence forces review 2022*. Dublin: Defence Forces Printing Press, 1–11.
Council of the European Union, 2014. European Union Maritime Security Strategy, 24 June.
Craven, J.P., 2001. *The silent war: the cold war battle beneath the sea*. New York: Simon & Schuster.
Davenport, T.M., 2015a. The high seas freedom to lay submarine cables and the protection of the marine environment: challenges in high seas governance. *American journal of international Law*, 112, 139–143.
Davenport, T.M., 2015b. Submarine cables, cybersecurity and international law: an intersectional analysis. *Catholic university journal of Law and technology*, 24 (1), 57–109.
David, R.R., 2022. Submarine cables: risks and security threats. *Energy Industry Review*, 25 March.
Department of the Environment, Climate, and Communications (DECC), 2020. *International Connectivity for Telecommunications - Public Consultation*, October 2020.
Department of the Environment, Climate, and Communications (DECC), 2021. *International connectivity for telecommunications consultation – key findings*.
Department of the Environment, Climate, and Communications (DECC), 2022. Review of the security of energy supply of Ireland's Electricity and natural gas systems consultation, 19 September 2022.
Dinmohammadi, F., *et al*., 2019. Predicting damage and life expectancy of subsea power cables in offshore renewable energy applications. *IEEE access*, 7, 54658–54669.
Drea, E., 2022. Ireland is Europe's weakest link. *Foreign Policy*, 8 November.
Dunley, R., 2023. Uncrewed naval vessels and the span of maritime tasks. *Marine policy*, 149, 1–7.
EU Commission, 2022. CORDIS. Distributed acoustic sensing for cable monitoring and surveying for offshore wind farms providing movement, depth, surface disruption and free-span readings. Available from: https://cordis.europa.eu/project/id/768328.

European Subsea Cables Association, 2023. Subsea cable security frequently asked questions. Available from: https://escaeu.org/faqs/subsea-cable-security.
Flynn, B., and Ó hUiginn, P., 2019. Environmental policy integration: innovation and change. *EPA Research Report*. EPA: Wexford.
Gallagher, C., 2021. Lack of sailors forces naval service to cancel patrol days. *The Irish Times*, 16 July.
Gallagher, C., 2022. British surveillance ship to monitor subsea cables in Irish economic zone. *The Irish Times*, 28 July.
Germond, B., 2014. Small navies in perspective: deconstructing the hierarchy of naval forces. *In:* M. Mulqueen, D. Sanders, and I. Speller, eds. *Small navies: strategy and policy for small navies in war and peace*. London: Routledge, 40–41.
Germond-Duret, C.V., and Germond, B., 2022. Media coverage of the blue economy in British newspapers: sea blindness and sustainable development. *The geographical journal*, 00, 1–11.
Government of Ireland, 2019a. *White Paper on Defence Update* 2019.
Government of Ireland, 2019b. *National Cyber Security Strategy 2019*-2024.
Government of Ireland, 2020. *Strategic Emergency Management Guideline 3 - Version 2 – Critical Infrastructure Resilience*.
Government of Ireland, 2022a. Government statement on the role of data centres in Ireland's enterprise strategy, July.
Government of Ireland, 2022b. Department of Defence Capability Review, April.
Government of Ireland, 2022c. *Project Ireland 2040: national marine planning framework*. Dublin: Department of Housing, Local Government and Heritage.
Guilfoyle, D., Paige, T., and McLaughlin, R., 2022. The final frontier of cyberspace: the seabed beyond national jurisdiction and the protection of submarine cables. *International & comparative law quarterly*, 71 (3), 657–696.
Hayes, J., 2008. A history of transatlantic cables. *IEEE communications magazine*, 46 (9), 42–48.
Hillman, J.E., 2021. *Securing the subsea network a primer for policymakers*. Center for Strategic and International Studies, March.
Ho, M., *et al*., 2020. Inspection and monitoring systems subsea pipelines. *Structural health monitoring*, 19 (2), 606–645.
Houses of the Oireachtas, 2021a. Naval Service. Dáil Éireann debate, 18 November.
Houses of the Oireachtas, 2021b. Telecommunications Infrastructure. Dáil Éireann debate, 13 May.
Houses of the Oireachtas, 2022a. Maritime Jurisdiction. Dáil Éireann debate, 6 October 2022.
Houses of the Oireachtas, 2022b. Priority questions. Dáil Éireann debate, 24 November.
Hughes, G., 2020. War in the grey zone: historical reflections and contemporary implications. *Survival*, 62 (3), 131–158.
Information Fusion Centre, 2023. About IFC. Available from: https://www.ifc.org.sg/ifc2web/app_pages/User/commonv2/aboutus.cshtml.
International Cable Protection Committee (ICPC), 2009. Submarine cable network security. Presentation to the Asia-Pacific Economic Forum. Workshop and Information Sharing on Submarine Cable Protection. Singapore, 13 April.
International Cable Protection Committee (ICPC), 2021. Government best practices for protecting and promoting resilience of submarine telecommunications cables. Available from: https://www.iscpc.org/documents/?id = 3733.
Irish Defence Forces, 2023a. The fleet. Available from: https://www.military.ie/en/who-we-are/naval-service/the-fleet.
Irish Defence Forces, 2023b. Fisheries Monitoring Centre. Available from: https://www.military.ie/en/who-we-are/naval-service/specialist-units/fisheries-monitoring-centre.
Irish Department of Defence, 2022. Building for the future – change from within: high level action plan for the report of the commission on the defence forces.
Irish Department of Defence, 2023. Ceremonial handover of two Inshore Patrol Vessels from the New Zealand Government to the Irish Government. Available from: https://www.gov.ie/en/press-release/2ae2a-ceremonial-handover-of-two-inshore-patrol-vessels-ipvs-from-the-new-zealand-government-to-the-irish-government.

Irish Department of Transport, 2022. The Irish Coast Guard. Available from: https://www.gov.ie/en/policy-information/eda64a-the-irish-coast-guard.
Jentoft, S., and Chuenpagdee, R., 2009. Fisheries and coastal governance as a wicked problem. *Marine policy*, 33, 553–560.
Kazaz, N., 2022. Are laws regulating subsea cables outdated? *SubTel Forum Magazine* 123, March.
Kenny, A., 2022. Concern over Ireland's ability to protect undersea cables. *RTE News*, 29 September.
Killeen, M. 2022. Ireland, and Iceland linked through new subsea telecoms cable. *EURACTIV.com*, 14 November.
Leahy, P., 2023. Ireland likely to join NATO project to protect undersea cables. *Irish Times*, 14 May.
Marine Institute, 2022. The map of Ireland is bigger than you think. Available from: https://www.marine.ie/site-area/news-events/news/map-ireland-bigger-you-think.
Maritime Area Planning Act, 2021. Number 50 of 2021.
Maritime Area Regulatory Authority, 2023. Ireland's new Maritime Area Regulatory Authority (MARA) is coming soon. Available from: https://maritimeregulator.ie.
Maritime Security Act, 2004. Number 29 of 2004.
Martin, A., 2022. Fishing vessel, not sabotage, to blame for shetland island submarine cable cut. *The Record*, 20 October.
McNamara, E.M., 2022. Ireland's defence deficit. *RUSI*, 21 December.
McNamara, E.M., 2022a. Evolving Irish neutrality: military opportunities and political obstacles. *RUSI*, 15 July.
Mooney, J., 2020. Russian agents plunge to new ocean depths in Ireland to crack transatlantic cables. *The Times*, 20 February.
Mooney, J., 2022. Kremlin homes in on EU's 'weak link'. *The Times*, 30 January.
Mueller, S.L., 2016. *Wiring the world: the social and cultural creation of global telegraph networks*. New York: Columbia University Press.
Mugg, J., Hawkins, Z., and Coyne, J., 2016. *Special report: Australian border security and unmanned maritime vehicles*. Canberra: Australian Strategic Policy Institute.
Mugridge, D., 2009. Malaise or farce - the international failure of maritime security. *Defense and security analysis*, 25 (3), 305–311.
Murphy, S., 2022. Ireland fires broadside at Russia over naval drills plan off coast - but lacks military muscle to do much else. *Sky News*, 24 January.
North Atlantic Treaty Organization (NATO), 2023. NATO stands up undersea infrastructure coordination cell. *NATO*, 15 February. Available from: https://www.nato.int/cps/en/natohq/news_211919.htm.
Office of Government Procurement, 2022. JN 841/2022 - MULTIBEAM ECHO SOUNDER.
O'Keefe, C., 2021. Navy chiefs issue security warnings over presence of 'foreign military vessels'. *Irish Examiner*, 20 November.
O'Keefe, C., 2022. Ireland 'obliged' to build naval capacity to protect underwater cables and pipelines. *Irish Examiner*, 4 October.
Olsen, J.M., 2022. Swedish navy sends special diving vessel to area of pipeline leaks. *Irish Examiner*, 3 October.
Patalano, A., 2023. Unseen but vital: Britain and undersea security. Council on Geostrategy, 8 March.
Permanent Structured Cooperation (PESCO), 2023. Critical Seabed Infrastructure Protection (CSIP). Available from: https://www.pesco.europa.eu/project/critical-seabed-infrastructure-protection-csip.
Phelan, C., 2023. Ireland to consider joining EU/NATO-led mission to protect undersea cables. *Irish Examiner*, 01 June.
Rode, P., 2017. Urban planning and transport policy integration: the role of governance hierarchies and networks in London and Berlin. *Journal of urban affairs*, 41 (1), 39–63.
SafeSeas, 2018. *Mastering maritime security: reflexive capacity building and the western Indian ocean experience*. Cardiff: Cardiff University.
Schaub Jr., G., Murphy, M., and Hoffman, F.G., 2017. Hybrid maritime warfare: building Baltic resilience. *The RUSI journal*, 162 (1), 32–40.

Speller, I., 2021. Commission on the Defence Forces. Public Consultation Response. May. Available from: https://assets.gov.ie/136077/aa60413b-17e9-4f09-bdd8-0839ecfd0b20.pdf.
Submarine Telegraph Act, 1885. Irish Statute Book, CHAPTER XLIX.
Swedish Armed Forces, 2023. The navy: fighting capability on, over and under water. Available from: https://www.forsvarsmakten.se/en/about/organisation/the-navy.
The Moscow Times, 2020. Ireland suspects Russian agents of inspecting undersea cables – the times. *The Moscow Times*, 18 February.
Till, G., 2014. Are small navies different? *In*: M. Mulqueen, D. Sanders, and I. Speller, eds. *Small navies: strategy and policy for small navies in war and peace*. London: Routledge, 21–33.
Trump, B.D., Hossain, K., and Linkov, I., 2020. *Cybersecurity and resilience in the Arctic*. Amsterdam: IOS Press.
UK Government, 2023. Joint Maritime Security Centre. Available from: https://www.gov.uk/government/groups/joint-maritime-security-centre.
UK Ministry of Defence, 2023. New UK subsea protection ship arrives into Merseyside. 19 January. Available from: https://www.gov.uk/government/news/new-uk-subsea-protection-ship-arrives-into-merseyside.
UN Convention on the Law of the Sea, 1982. (UNCLOS).
Whittaker, A., 2020. Connected Ireland: how subsea fibre optic cables help to drive our social, economic and industrial development. *Engineers journal*, 13 November. Available from: https://www.engineersireland.ie/Engineers-Journal/More/Sponsored/connected-ireland-how-subsea-fibre-optic-cables-help-to-drive-our-social-economic-and-industrial-development.
Wivel, A., and Oest, K.J.N., 2010. Security, profit or shadow of the past? Explaining the security strategies of microstates. *Cambridge review of international affairs*, 23 (3), 429–453.
Wu, H. 2023. Taiwan suspects Chinese ships cut islands' internet cables. *Associated Press News*, 8 March.
Xiang, X., *et al*., 2016. Subsea cable tracking by autonomous underwater vehicle with magnetic sensing guidance. *Sensors*, 16 (8), 1335.