Inaugural Symposium on Subsea Cable Security and Resilience

10-12 October 2024, Valentia Island Transatlantic Cable Station, Valentia Island, Co. Kerry, Ireland

A Report of Proceedings

VALENTIA TRANSATLANTIC CABLE FOUNDATION

Preface

Organising an international event on a topic of significant global interest at a nineteenth century telegraph station on an island off the south coast of Ireland during the month of October is no easy feat. Yet we proved it is possible. For this we are enormously grateful to our hosts, the Valentia Island Foundation, the Government of Ireland, Kerry County Council, the European Subsea Cables Association (ESCA), the International Cable Protection Committee (ICPC) and the Symposium sponsors listed below for their support and participation in the event. Then Tánaiste Micheál Martin's keynote speech and the attendance of officials from across different government departments are a clear indication of the importance of the topic.

Thank you to all the presenters, speakers and moderators from across academia, industry and government who travelled from near and afar to trace the sometimes-fitful journey of submarine cables from their first trans-Atlantic crossing from Valentia Island to Heart's Content to their massive spread across the globe today. Their expert contributions throughout the three days and the banter at night contributed to the rich content and uniqueness of the event.

Hats off to Professor Chris Morash for his memorable evening keynote "A Momentary Sense of Wonder': A Message from the Transatlantic Telegraph of 1858"; to Dr. Donard De Cogan for providing historical context to the Symposium's location and for sharing the captivating story of the first transatlantic cables; and to Derek Cassidy, Séan Walsh and Tara Bishop for their live demonstration, in Morse Code, of the first ever message transmitted between the Valentia Island and Heart's Content telegraph stations that same year.

Huge thanks also to Robert McCabe, Brendan Flynn and Kent Bressie for their role on the CfP panel and, importantly, to Jonas Franken, Lane Burdette and Cian Fitzgerald for their important contribution to the drafting of this report.

Last and certainly not least, a very special thanks to the staff at the Valentia Island Cable Station, the Royal Hotel at Valentia Island, the Heritage Centre, the Church of St John the Baptist and to the communities of Valentia Island and Portmagee for their exceptional hospitality (and for organizing the fantastic weather!). To each and every one of you, go raibh míle maith agaibh, thank you!

The Organising Team

Camino Kavanagh, Symposium Chair
Leonard Hobbs, Chair, Valentia Transatlantic Cable Foundation
Sandra Delany, Aqua Comms
John Wrottesley, European Subsea Cables Association (ESCA)
Nicole Starosielski, University of California at Berkeley

Supported and sponsored by

analysys mason

An Roinn Gnóthaí Eachtracha agus Trádála
Department of Foreign Affairs and Trade

An Roinn Cosanta
Department of Defence

AQUACOMMS

Aurora TELECOM

EUROPEAN SUBSEA CABLES ASSOCIATION

IDA Ireland

International Cable Protection Committee

PHILIPLEE

Table of Contents

6 Acronyms and Definitions

8 Introduction

10 Panel 1: Subsea Cable Security and Resilience: Learning from the Past

14 Panel 2: The Present: Getting Subsea Cable Security and Resilience to Meet

19 Panel 3: Subsea cable incidents: data collection, reporting and response

24 Roundtable 1 Operating in a Heightened Geopolitical Environment

28 Panel 4: Fault Prevention and Cable Repair Ecosystem

32 Panel 5: The contribution of technology to cable security and resilience

36 Roundtable 2: Subsea Telecommunications Cable Policy and Regulation for the Future

39 ANNEX 1: Symposium Agenda

Acronyms and Definitions

AIS	Automatic Identification System: A vessel tracking system used to monitor and manage maritime traffic.
CPEI	Cable Projects of European Interest: EU-supported projects aimed at enhancing subsea cable infrastructure resilience and security.
CER Directive	Critical Entities Resilience Directive: An EU directive focusing on the resilience of critical infrastructure, including subsea cables
CfP	Call for Presentations
DAS	Distributed Acoustic Sensing: A technology that transforms optical fibres into sensors for detecting underwater activities, seismic activity, and potential security threats.
EC	European Commission: The executive branch of the European Union responsible for implementing laws, policies, and regulations.
EEZ	Exclusive Economic Zone: A maritime zone extending up to 200 nautical miles from a country's coast, granting it special rights over marine resources.
ESCA	European Subsea Cables Association: An industry body representing submarine cable operators, supporting best practices for security and resilience.
EU	European Union: A political and economic union of 27 European countries.
GDPR	General Data Protection Regulation: An EU regulation governing personal data protection and privacy.
GMA	Ghana Maritime Authority: A regulatory body overseeing maritime activities and subsea cable protection in Ghana.
HF Radio	High-Frequency Radio: A long-range communication system often used for backup in maritime and emergency scenarios.
ICPC	International Cable Protection Committee: A global organisation dedicated to protecting and managing submarine cable infrastructure.
IMO	International Maritime Organization: A UN agency that regulates shipping, maritime safety, and environmental protection.
ITP	International Tailored Partnership Programme (NATO): A NATO initiative for engagement with non-member states on security matters, including maritime security.
KIS-ORCA	Kingfisher Information Service - Offshore Renewable & Cable Awareness: A system that provides updated subsea cable maps to marine users to prevent damage.
MAPA	Maritime Area Planning Act: Irish legislation governing seabed usage, marine planning, and cable permitting.
MARA	Maritime Area Regulatory Authority: An Irish government agency responsible for managing maritime area activities, including subsea cables.
NATO	North Atlantic Treaty Organization: A military alliance between 31 countries, including many EU members, focused on collective security.
NIS2	Network and Information Security Directive 2: An EU directive enhancing cybersecurity and resilience of critical infrastructure, including subsea cables.
NOC	Network Operations Centre: A facility responsible for monitoring and managing telecommunications networks, including submarine cables.
OFDR	Optical Frequency Domain Reflectometry: A fibre-optic sensing technology used for detecting faults or disturbances along subsea cables.
PoC	Point of Contact: A designated individual or entity responsible for coordination and communication.
SoP	State of Polarization: A technique used in optical networks and sensing systems, including for monitoring

	subsea cables
SMART cables	Science Monitoring and Reliable Telecommunications (SMART) cables
UNCLOS	United Nations Convention on the Law of the Sea: The international legal framework governing maritime rights, including protections for submarine cables.
VMS	Vessel Monitoring System: A satellite-based system used to track and manage fishing and commercial vessel activities.

Introduction

The Inaugural Valentia Island Symposium on Subsea Cable Security and Resilience, held from October 10-12, 2024, brought together Irish and international experts from industry, academia, and government to address critical issues related to submarine telecommunications cables (also referred to as subsea cables throughout the report). Hosted at the historic Valentia Island Transatlantic Cable Station, a symbol of global communication and innovation, the Symposium provided a unique setting to reflect on the historical, political, social, economic, and technological dimensions of subsea cable security and resilience.

Over three days of presentations, thematic panels and side events, recognized experts in the field examined historical continuities and discontinuities in key security and resilience questions; how security and resilience come together in national policy; current policy and practice in identifying and responding to subsea cable-related incidents; how industry and government are adapting to the current geopolitical environment; core characteristics of the cable repair eco-system and related challenges; technology's contribution to security and resilience of the systems; and current and future policy and regulatory issues.

Several recurring themes central to the discussion on subsea cable security and resilience are evident. Principle among them is the growing complexity of the regulatory environment at a time when, for both resilience and security purposes, regulation needs to be more streamlined and predictable, attuned to shifting cable ownership models, as well as better coordinated and harmonised across connected countries, while also meeting one of its primary aims, which is to prevent and mitigate risks that could negatively impact individuals, communities, or entire societies. Many governments are working towards these goals within a broader framework of critical infrastructure protection.

Second, as in the past, geopolitical tensions affect the subsea cable ecosystem. They influence the geographies of the physical network and spill over into regulation and an ever-broadening number of policy areas, at national, regional and international levels. Ensuring the availability of the systems and of fleets and supply chains is a concern of both industry and government. It requires various modes of public-private engagement at sea and on land and should be a priority.

Third, the subsea cable industry owns and operates most cable systems. Owners and operators are expected to ensure resilience

across a cable system's life cycle. At the same time, governments are responsible for national security and have a duty to their citizens to ensure delivery of essential services and functions. Public-private engagement is key for reaching common understandings on how these different but often overlapping duties can be met whether in peacetime, in crisis or in conflict.

Fourth, technology plays a critical role in both public and private efforts to ensure the resilience and security of subsea cables systems. Technologies such as Distributed Acoustic Sensing (DAS) offer significant advantages for environmental monitoring, disaster early warning and for more defense-related situational awareness, particularly when combined with other technologies. Legal and regulatory questions regarding their use within and beyond national jurisdictions need to be addressed, including how they may be qualified in the event of hostilities and what this would mean for cable operators.

Lastly, the Symposium shed light on the temporality and spatiality of many of the subsea cable resilience issues discussed over the three days. Temporal aspects include the lengthy history of submarine transmission technologies, response times for repairs, aging repair assets and workforce and the longevity of the infrastructure. Spatial aspects include jurisdictional questions relevant to addressing cable damage, the monitoring range of technologies such as DAS, the intensifying competition for the use of the seabed and the marine space. This "spatial squeeze" also has its geopolitical underpinnings, as do a growing number of other cable related matters.

These and many other issues discussed herein require sustained attention over the coming years. Hosting them at venues such as the Valentia Island Telegraph Station remind us of our shared heritage as well as the importance of history when addressing the problems of today.

What follows are key takeaways and summaries of the main panel discussions. A full Agenda covering the three days of deliberations can be found in the Annex. We welcome any comments via the following email address: info@ValentiaCable.com

Panel 1

Subsea Cable Security and Resilience: Learning from the Past

The first panel of the Symposium examined the historical trajectory and the geopolitical significance of submarine cables through the lens of politics, economics, place and people.

Key Takeaways

- Submarine telecommunications cables have been a cornerstone of global communications since the 19th century. The past 150 years has seen significant changes in their underlying technology, ownership and use. The evolution from telegraph, to coaxial, to fibre-optic cables has significantly increased capacity, and global dependence on subsea systems.
- Ownership has transitioned from private funding in the 19th century to significant government involvement in the mid-20th century, and back to private sector dominance in recent decades. Ownership structures and dependencies strongly influence security prerogatives, as well as government action where regulation, defence and diplomacy are concerned.
- Most incidents of cable damage stem from commercial activity or natural events. Nonetheless, submarine telecommunications cables have featured strongly in international politics and in warfare at different moments in history. State-backed sabotage and espionage at sea, at cable landing stations, or at terrestrial points of presence have remained persistent risks, even if technological developments are making some of these activities more difficult. Cyber security of specific system elements and components, supply chain security as well as dis/misinformation campaigns were highlighted as additional risks
- Redundancy concerns have long historic roots. Today, network-level redundancy and geographic diversity help to mitigate disruptions caused by outages. The ability to repair cables swiftly is vital, although there are concerns over the availability and ageing of cable repair fleets and workforce shortages. Maintenance agreements are critical but require investment and protection. Satellite connectivity can also provide backup in the event of disruption – most notably for remote and under-served island communities, though the capacity of such satellite systems is exponentially less compared to subsea cables.
- While there are concerns around the charting of subsea cables from a security perspective, charting enhances awareness for other sea users and reduces accidental damage from fishing and anchoring.
- Trusted and sustained partnerships between the public and private sectors are essential for addressing shared challenges like personnel turnover, political changes, and resource constraints.
- Sustained collaboration and updated regulatory frameworks are equally critical to adapting to shifts in cable ownership and architectures, and to technological and geopolitical challenges.
- Many of the issues affecting subsea cables and shaping resilience efforts have a long history. Recording and exchanging knowledge and lessons across different generations of industry and government representatives can contribute to problem solving today.

Main Discussion Points

The very location of the symposium – the Transatlantic Telegraph Station on Valentia Island – and the first cables that landed there play an important role in the history of submarine cables. The Island's proximity to Newfoundland in Canada made it an ideal site for establishing the first transatlantic communication connection in the 19th century, minimizing cable length and costs.

Historically, the decision to install and operate submarine telegraph cables depended on scientific and technological developments, as well as on geographic, economic and political stability. For instance, in Ireland, poor economic growth, domestic political unrest following independence, and the country's policy of political neutrality and non-NATO status during the Cold War likely contributed to cable landing decisions, evidenced by the fact that in 1984, no modern cable systems landed in Ireland. In the latter years of the Cold War these concerns abated in tandem with the privatisation of the infrastructure, as evidenced in the number of cables landing in or planned to land in Ireland today.

The economic well-being of a country also dictated how much traffic was generated. For instance, much of the early traffic routing through Valentia Island was communications on financial markets and other news. Telegraph messaging was largely inaccessible to the people of Ireland, then a colony. After World War II, governmental and military communications dominated global submarine telegraph cable use. However, the second half of the 20th century, which saw the technology transition from copper to coaxial to high-capacity fibre optic cables, private communications over the systems grew significantly. Today, most of the fibre optic demand is internet-based, including machine-to-machine communications, marking an inflection point in the evolution of submarine cable systems.

Historically, early submarine telegraph cable builds were privately funded, with governments becoming more involved during the mid-20th century. In recent years, the balance has shifted back to private sector financing with ownership of subsea cables transitioning from governments and national monopolies to international consortia and private companies. Governments today are refocusing, setting strategic priorities and ensuring a say in security and resilience through regulation, national preparedness and international partnerships. As in the past, foreign ownership of cables or specific equipment and components is under increased scrutiny, often manifest in licensing processes and decisions.

Concerns about state-backed sabotage and espionage (at sea, at the cable landing station or at the terrestrial point of presence) have remained a constant throughout history, and the threat of such actions has resurfaced in recent years. As with other critical infrastructure, the relevant software, hardware, systems and components of subsea cables are vulnerable to cyber threats involving States or their proxies. Misinformation and disinformation relevant to recent incidents is another challenge. Subsea cables are inherently vulnerable, and it will never be possible to fully secure them. Security of the systems is also intrinsically tied to ownership structures, although such distinctions are harder to make today. As in the past, governments use regulation to exercise control over the infrastructure, although the underlying normative and diplomatic framework driving government action stems from the nineteenth century and requires updating. Throughout history, States have also used the tool of diplomacy to exercise control over submarine cables, whether it be to influence how the systems were qualified and disposed of in post-war negotiations; to shape decisions over cable landings; and to ensure or prevent access to strategic geographies and access to information. Securing access for repair in the Red Sea is a recent example of behind-the-scenes diplomacy in action.

Concerns regarding redundancy have also been a constant throughout history. Modern redundancy systems minimize disruptions caused by cable outages through swift rerouting of data traffic. Network-level redundancy and geographical diversity are a key focus for industry actors today. Overall subsea cables resilience also extends to the ability to repair cables quickly and having sufficient cable supplies and repair ships available in strategic locations, and trained crews. Today, both industry and governments share concerns about cable repair fleets and an aging workforce, as well as increasing delays in the time taken for repairs to commence. These delays differ across countries and regions and can be due to a range of factors, including weather, water depth, location of fault (transit time), availability of vessel, availability of spares, permitting requirements or restrictive policies which may be unrelated to subsea cable policy, but still can have unintended consequences to create barriers to fast repair response.

Existing private and zone maintenance agreements have served the industry well to date yet the high cost of maintaining these vessels and the specialised technology and crew requires attention. In historically contested maritime regions like the Red Sea, repair operations face additional, often unexpected, challenges that also require attention. As in the past, in addition to the latter, it is important to ensure independent backup systems for critical services and functions. In the 1960 and 1970s, HF radio and microwave links provided low-bandwidth, high latency redundancy options. Today microwave links along with satellites serve a similar purpose and need to be protected. However, the capacity of these systems to carry data is exponentially less than subsea cables.

Charting of submarine cables for awareness is another issue that has deep historical roots and linked to safety at sea considerations. Publicizing cable routes helps prevent the main causes of accidental damage by activities such as fishing or anchoring, however there can be a perception that such levels of transparency potentially expose the systems to increased vulnerability to targeted attacks. Some governments are looking at cable corridors, cable protection zones and other such protection measures to reduce risk, yet geographical clustering can also concentrate risk. In this regard, there is a need to enhance awareness and collaboration among key stakeholders to reduce common risks and agree on what information needs to be shared and how to securely share it.

Awareness raising around today's subsea fibre optic systems and their importance to society's functions is as key now as it was over a century ago when the submarine telegraph industry engaged in efforts to convince parliamentarians and congressional committees of the importance of the technologies.

Panel 2

The Present: Getting Subsea Cable Security and Resilience to Meet

This second panel examined approaches to managing risks to subsea cable systems, assessing ways to ensure a better balance between government and industry approaches to security and resilience and ensure they are mutually beneficial and do not create adverse consequences.

Key takeaways

- While age-old resilience challenges such as cable damage caused by human activities persist, the current geopolitical context is also presenting new risks that both government and industry will need to manage.
- Greater stakeholder collaboration and data sharing can ensure more rapid determination of intentional activity, even if deliberate grey-zone actions, such as using commercial vessels to cut cables, are difficult to attribute. While developing their approaches to such hybrid risks, governments need to also address existing challenges affecting day-to-day operations in the maritime domain.
- Damage to cables at sea is not the only concern of governments. A more systemic approach to risk would cover cybersecurity, supply chain security and procurement issues, amongst other. This can result in an overly complex regulatory and operational environment requiring significant engagement across government and with industry.
- Government and industry often have different perspectives of risk, but they share key resilience imperatives, including prevention and rapid recovery. Effective crisis management requires aligning approaches within and across connected countries, as well as leveraging lessons from incidents.
- Dialogue amongst a wider variety of stakeholders on security and resilience challenges and on how to best balance security and resilience is positive. However, it has its limitations. Working towards common understandings and ensuring greater conceptual clarity and coherence around threats and risks should be a priority.

Main Discussion Points

The panel discussion “The Present: Getting Subsea Cable Security and Resilience to Meet” emphasised the changing focus on subsea cables as critical infrastructure. Core questions discussed included how to best balance government and industry prerogatives when strengthening the security and resilience of such critical infrastructure, and how to avoid over- or under securitisation of national approaches.

The maritime environment is becoming increasingly complex and in many maritime regions, the number of seabed users continues to grow. This creates resilience challenges for the subsea cable industry and for governments. Against this backdrop, the geopolitical context is driving new national and international security concerns which governments need to attend to. These security concerns also affect industry.

Approximately 80% of subsea cable breakages result from fishing and anchoring each year. The remaining causes of damage result from natural hazards, abrasion and equipment failure. Traditional ways to mitigate against these kinds of incidents includes, inter alia, route design to mitigate risks, physical protection such as burial, AIS/VMS monitoring and ensuring a robust repair eco-system. Technologies such as Distributed Acoustic Sensing (DAS) can also contribute to protecting the systems, although it raises questions about how the systems will then be qualified from a legal and regulatory perspective. Engagement with the fishing industry and charting of cables for awareness of fishers is another approach, also linked to safety of life at sea and protection of subsea cables.

Nonetheless, the changing geopolitical environment has created a different risk perception in some regions, including the threat of sabotage and other kinds of cyber, physical and supply chain threats to the systems involving state and non-state actors. The challenge will be ensuring that subsea cable protection does not become an overly securitised issue in national policy and undermine resilience.

On cable damage, the use of commercial vessels (trawlers etc.) to deliberately cut subsea telecommunications cables and other undersea infrastructure in peacetime could be a tactic in a broader menu of grey zone activities. Attributing these kinds of hybrid actions is very difficult. In some situations, the actual location of the cable and its possible strategic utility can be a good indicator as to whether an incident was an act of sabotage or not. To determine whether cuts were accidental or intentional it is essential to examine the cables directly and review other sources of information such as AIS monitoring and VMS data to review vessel activity at the fault location around the time of the incident. This is complicated by the fact that AIS systems – the use of which is mandatory – are often turned off (or down) or otherwise manipulated by fishing vessels to avoid detection or prevent competitors from monitoring their fishing grounds. Moreover, their use – AIS in particular- is not effectively enforced. For its part, VMS data is often hard to acquire with data protection regulations such as GDPR often cited as a reason, although it can usually be made available in the event of legal action being taken. The plausible deniability driver of hybrid operations resulting in cable damage poses political and security challenges, although efforts are underway in certain waters to 'deny the deniability". More detailed information on how governments respond to hybrid activity is not always in the public domain.

For industry, regardless of the cause of cable damage, the cable still needs to be repaired, and service restored. The response times for repair vessels and the role of communication are essential in this regard. The changing nature of the subsea cable industry with hyperscalers building their own cable systems brings changes to some of the long-standing industry dynamics and can introduce new opportunities and risks. Some of the greater risks and challenges facing the industry that can have real impacts and reduce national resilience for countries includes excessive permitting and regulation, some of which stem from national security concerns and broader geopolitical risks, as evidenced in increased delays for landing and repair permits in some jurisdictions. The extra-territorial reach of some countries' legislation is also a risk.

Governments are just as concerned about physical and cyber security risks to the systems on land as they are to sabotage at sea. Espionage is a particular problem, but it is often discussed in relation to what was possible in earlier generations of subsea communications technologies. Most successful examples of cable tapping at sea (e.g. Operation Ivy Bells) occurred in the period of copper or coaxial cable systems. Today's fibre optic systems make cable tapping much more difficult and significantly reduce the possibility of such actions going undetected under the sea, and the primary risks around espionage are terrestrial rather than subsea.

In the EU context, governments are grappling with a shifting regulatory environment, with new regulations (e.g., NIS2) replacing older ones (e.g., Electronic Communications Code) aimed at dealing with some of these risks. Government and industry often have different perspectives of risk but share common resilience objectives. For a company or consortium of companies that own a cable, the risk to that cable is solely associated with ensuring traffic can be rerouted in the event of an incident. For governments, there is an overarching responsibility towards citizens and ensuring the delivery of key services. This means not just looking at the primary effects of cable damage, but secondary and tertiary effects.

Recent incidents have increased awareness across stakeholders of cable damage. When several cables are cut at the same time, the chance of full or partial service disruption increases. There are many examples of events that have resulted in the simultaneous break of numerous cable systems, leading to widespread disruption (e.g., the 2006 earthquake in Taiwan; the separate incidents of cable breaks that occurred in 2008 due to anchor drag or anchor drop in the Middle East and in the Mediterranean, or the 2016 incident in the Channel between the UK and France). In this regard, there are important lessons to be drawn from countries that have experienced and are on constant alert for natural events such as volcano eruptions, earthquakes and triggers of turbidity currents and on the role of technology in early warning. Industry's approach to cable protection and route engineering is equally important in this regard.

Recent incidents can serve as a basis for both government and industry to collaborate to assess risk, establish crisis management protocols and procedures and cooperative mechanisms. Alignment of approaches across connected countries is key and can allow for more agile and streamlined responses to incidents.

In this regard, many of the on-going conversations between connected countries are centred not just on managing risks to the cable *per se,* but also on managing other kinds of risks such as cyber and economic security risks relative to supply chains, system equipment and components, and maintenance and repair capabilities. These kinds of exchanges on risk management and

relevant crisis management responses can help ensure governments are better equipped to deal with incidents and prevent outages, especially when a society's vital functions are affected. Designated points of contact and systematic and secure data sharing across key stakeholders is also key to risk management. There is significant experimentation underway to identify the best means for information and intelligence sharing across countries and between government and industry. In Ireland, for example, the National Cyber Security Centre has established a number of coordination and response groups with different industry sectors to share information on a quasi-formal basis and ensure relevant points of contact in government and the different industry sectors are in place in the evident of a cyber incident affecting any given operator. The forthcoming maritime security strategy being prepared by Ireland will also be a vehicle for greater coordination on risks and responses to critical infrastructure in both maritime and onshore spaces.

Subsea cable protection is not a new topic for the industry, but the heightened profile from media coverage of cable damage since the 2022 Nord Stream pipeline explosions has led to increased government and public awareness. The greater attention being paid to the protection of subsea cables by governments is positive, although the proliferation of panels and fora discussing subsea cables can also generate challenges around sourcing the expertise required to discuss the nuanced risks to which subsea cable telecommunications infrastructure are exposed. There are also risks around group think, observation and confirmation bias and dilution of competences. In this regard, building an objective technical basis and reaching coherent and common understandings of resilience and risk is key.

The role of academia in discussions on security and resilience is important. Generally unburdened by political and commercial interests, they can play an objective role in fielding questions, providing historical context to contemporary concerns, producing options for how to approach certain issues, modelling approaches to complex problems, developing content for exercises, including tabletop exercises, monitoring implementation of national policy and strategy and so forth. As evidenced in this Symposium, bringing together academia, industry and government can produce positive results and should be sustained.

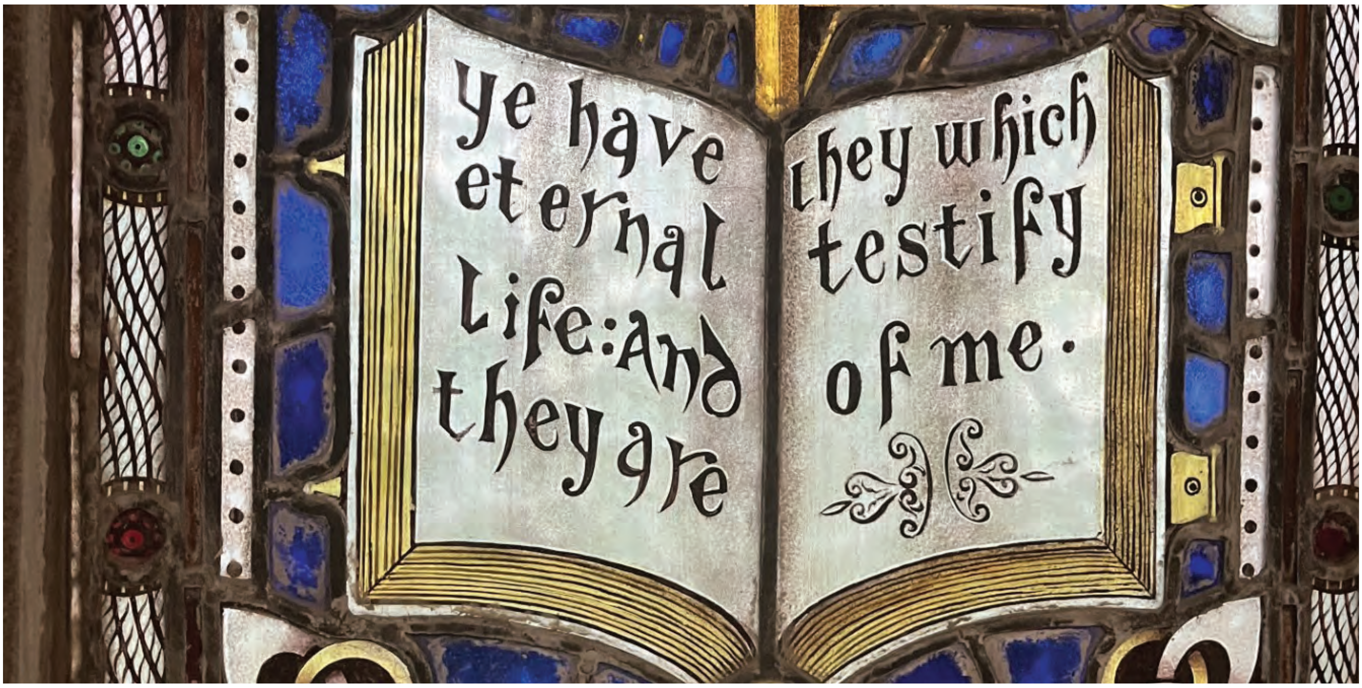
Panel 3

Subsea cable incidents: data collection, reporting and response

The panel on "Subsea cable incidents: data collection, reporting, and response" examined different aspects of cable damage at sea, including how such damage is assessed and how repairs are conducted; and the different roles and responsibilities of government in ensuring cable security and resilience.

Key Takeaways

- The frequency and duration of repairs vary significantly across regions. Government authorities can help minimize repair times through effective policy, streamlined permitting and targeted exemptions, pre-approval or expedited permit processing for cable repair ships. National security prerogatives and the current geopolitical context could potentially create more barriers. Balancing efficiency and security in licensing, permitting, and critical infrastructure protection regimes is crucial to avoid unintended delays.
- While the subsea cable repair ecosystem faces certain challenges, such as aging workforce and fleets, personnel and skills shortages, it remains confident in its ability to carry out timely repairs in peacetime, if permits are exempted, pre-authorised or issued quickly.
- The cable industry is expected to be able to ensure business continuity in the event of cable faults, which by logic, would include sabotage. Systematic data gathering over the years has identified trends in cable faults, which serves as a guide for the repair eco-system. Industry is also aware that unintended events can always happen. In this regard, preparing for the unexpected, including through engagement with government is key to determining roles and responsibilities in the event of such incidents.
- Governments, too, are increasingly expected to prevent and respond to serious incidents affecting subsea cable systems. Engaging with industry is key to understanding opportunities and limitations of proposed national security driven interventions, and for identifying solutions to those issues – such as the most common causes of cable damage - that can be advanced in parallel.



Main Discussion Points

As in earlier panels, the discussions highlighted the frequency of subsea cable outages and how statistics on cable damage can vary significantly across geographies in terms of cause, and also time to repair. For instance, shallow waters with dense fishing and shipping activity tend to suffer from regular baselines of faults, although existing cable protection measures and strategies help to mitigate them. The variation in frequency of cable faults as well as redundancy levels inform needs and requirements of the repair industry. Cable repair activities can vary in duration depending on several factors such as water depth (deep water, shallow water or shore end), location of fault (transit time), availability of vessel, availability of spares, permitting, etc. A typical cable fault assessment and repair process involves several steps:

A fault is alerted to the network operations centre (NOC). Initial diagnostics are carried out to determine if the fault is in the transmission equipment, in the front haul or if it is in the submersed part of the cable.

Following from that initial assessment, more detailed diagnostics help determine if it is either one of two primary types of cable fault: a full fibre break or a shunt fault. In this regard, it is worth mentioning that a fibre break tends to be pretty evident since the cable is severed resulting in full loss service is lost. A shunt fault is when the outer insulation of the cable has been damaged, resulting in a short circuit of electricity and can be more difficult to confirm. With shunt faults typically service can be kept on the system. Other factors that are considered in damage assessment include the location of the fault, the seabed conditions, the occurrence of natural events (e.g., seismic activity or storm events), or possible component or equipment failures. Operators will check their AIS monitoring systems to determine if vessels were in the vicinity of the cable.

The next step involves reporting the fault to authorities and customers, with obligations varying by jurisdiction. A vessel will then be called out and mobilised, either through private or Maintenance Zone agreements. Maintenance Zones involve multiple cable owners paying to have a vessel on standby or ready to depart for a cable repair within 24 hours, 7 days a week, 365 days a year. This self-insurance model contrasts with the offshore energy sector's insurer coordination model. It places more responsibility and coordination effort on cable operators in this third step – but significantly improves emergency response and is a fundamental pillar of subsea cable resilience. In the event of multiple cable faults occurring at the same time, the agreements denote how prioritisation within private or zone agreements occurs. Decisions are informed by dialogue between cable owners, meaning that the prioritisation schema is not always rigid.

Once a cable ship has been mobilised, it will depart for the repair ground. Due to the strategic geographic locations of repair ships, average transit times are estimated to be usually under two weeks, but this can vary by geography. Sometimes permitting poses significant delays, and can have the unintended consequence of slowing down, or in some instances preventing repairs from commencing in a timely manner.

Some countries provide specific exemptions or expedite the permitting process for cable repair vessels operating in their waters, leading to a much quicker response time. One example is the UK which has one of the highest fault rates in the world due to dense shipping, fishing and a high number of cables – but has one of the most rapid response times. Cable repair is specifically exempted through legislation to allow repairs to commence, with notification to authorities required within 24 hours of the repair commencing. This means that the vessel could already be on site undertaking the repair prior to the notification being made. Some countries require permits to be obtained, although some of these may ensure the permitting process is timely. Some countries may have domestic shipping policies that can complicate or delay repairs from commencing.

Straightforward and typical cable repairs take 5-7 days to complete on average from arrival on repair ground to deploying the cable following repair (depending on weather or other operational conditions which can extend repair times). For deep water operations, or complex repairs (for example where large sections are damaged following a landslide the time period both for planning and repair can increase.

The general trend for subsea cable repair is positive. Despite the number of subsea cable kilometres increasing from approximately 1 million kilometres in 2014 to 1.7 million kilometres in 2024, the actual number of faults per year remains relatively static at approx. 150-200 cable faults per year. This means that the fault rate per kilometre of laid cable is declining in recent years. This could be attributed to improved installation methods, including deeper cable burial, advanced monitoring, high-resolution surveys, greater cable awareness through charting, and improvements to cable route design.

Nonetheless, cable repair commencement time is increasing in some regions. Delays to repair commencement represents one of the most significant challenges to subsea cable resilience – and these are largely preventable. Different potential forms of state intervention in the repair market were discussed by this panel, although not explored in detail.

Geopolitical tensions are driving concerns in some countries about the companies they can trust, potentially affecting future repair operations. Some states are also considering different investment models to fill potential capability gaps. Questions regarding potential pressures on the cable repair eco-system during crisis could benefit from deeper discussion amongst key stakeholders. This could include state or public-private investment in repair resources or in pooling capabilities.

While recognising that subsea cable owners and operators are responsible for subsea cable operations and maintenance, the panel discussion also discussed roles and responsibilities of governments in subsea cable security and resilience matters. For instance, physical protection at sea often involves defence departments and the deployment of naval capabilities in addition to law enforcement; the cybersecurity of system equipment and components would fall under national cyber security entities and requirements for redundancy and capacity could be specified by a telecommunications regulator or may fall under national preparedness legislation.

In the context of Ireland, efforts are underway to finetune roles and responsibilities of different government actors and determine where information sharing is most needed across government and with industry. Following public consultations, efforts are also underway to align Ireland's subsea cable strategy with EU policy to address vulnerabilities and increase resilience through better connectivity and redundancy. The country's plan-led approach to future connectivity will help determine where more connections are needed and ensure alignment with other plans for the seabed and with other seabed users.

In the context of Ghana, the Ghana Maritime Authority's (GMA) plays an important role in overseeing maritime activities and protecting subsea cables. It acts as a liaison between cable operators, sea users, and government departments to enforce laws and raise awareness of cable safety and is advocating to raise awareness amongst other seabed users, and to improve coordination and response to cable damage incidents. Ghana has specific legal protection zones around cables to prevent fishing and anchoring incidents.

Governments can attract cable projects through streamlined permitting processes and other incentives. Publicly funded schemes such as the EU's Cable Projects of European Interest (CPEI) can support redundancy projects where market failure has been identified.

As in other panels, unpredictable and lengthy permitting processes across regions and lack of investment in new systems was a common theme in terms of the potential to undermine resilience objectives. Resolving these issues and ensuring more streamlined policies and active engagement between governments and industry can help attract investment and create robust, resilient systems to meet current and future demand.

Lastly, the panel discussed the importance of cross-sectoral engagement in the context of the increasing seabed development and the rapid expansion of offshore wind and other marine industries. As more industries and nations rely on subsea cables for telecommunications and energy as well as other seabed infrastructure, improved coordination across sectors, between governments, private companies, and other seabed users is essential to ensure that cable routes are not blocked (route foreclosure) and that repairs remain technically feasible as sufficient separation is needed from other seabed assets in order to recover cables for repair. The increase in human activity on the seabed and in the oceans also poses a greater risk of anthropogenic damage and conflict between sea users (dropped objects, unknown systems, inadvertent interactions during construction). These can only be mitigated through coordination and communication. Building on this, differing regional approaches can offer distinct perspectives on how to manage and regulate these spatial challenges, for example by the formation of cross-sectoral and multi-disciplinary expert groups, or use of existing monitoring architectures and data sharing platforms.

Roundtable 1

Operating in a Heightened Geopolitical Environment

The first RoundTable of the Symposium considered a range of geopolitical factors affecting subsea cable systems. Amongst other, it examined some of the drivers of current geopolitical tensions, as well as some of the levers that can facilitate a more integrated or coordinated approach to security and resilience efforts.

Key Takeaways

- The importance of subsea cables has surged on political and security agendas due to geopolitical developments and events like Nord Stream. Ensuring holistic and coherent approaches to subsea cable security and resilience is key. This includes clarifying roles and responsibilities across government agencies and with industry and making smart investments in capabilities.
- Shared awareness and understanding between government agencies, industries, and academia are critical to addressing maritime and subsea cable challenges. Enhanced data-sharing, leveraging fibre-sensing technologies (like DAS, SOP, interferometry), and fostering collaboration through forums and symposia are essential.
- There are gaps between national policy aims and the actual ability to respond with appropriate capabilities, as well as between the nature of the problem (e.g., accidental vs. malicious damage) and government responses.
- Balancing responses to high-impact, low-probability sabotage events and lower-impact, high-probability incidents remains a key challenge for governments and industry alike.
- Timely repairs can deter sabotage and minimize disruptions, but permitting delays imposed by governments can hinder operations.
- Repairs in conflict zones like the Red Sea, highlight challenges related to operating under live-fire conditions, legal issues and ensuring personnel/vessel safety.
- A maritime skills gap across government, academia, and industry poses a challenge to building capacity and ensuring subsea cable maintenance. Such challenges are more evident in situations of crisis.

Main Discussion Points

Political attention to subsea cables and their vulnerabilities is higher now than any other time in the last few decades. Much work is underway to define the different problems belonging to defence, law enforcement, diplomacy and the commercial domains and determine how these are brought together under coherent strategies and national preparedness frameworks.

On diplomacy: Indications of the importance of the topic on the international stage include 1) the Statement on Subsea Cable Security and Resilience presented at the 79th annual United Nations General Assembly in September 2024; 2) the range of new and updated EU instruments and strategies; 3) the recently-established International Advisory Body on subsea cable resilience jointly led by the ITU and the ICPC; and 4) the different NATO initiatives launched since the Nord Stream incident in 2022, to name but a few. That such a flurry of activity has happened is not entirely novel. Indeed, it tends to happen when new security issues emerge on the agenda. In this regard, there are many similarities with how governments approached cyber security issues almost two decades ago. The fact that subsea cable security and resilience has come up the policy agenda so rapidly is an indicator of how much it matters to governments. For all countries, this level of attention provides an opportunity to look at their position on the topic and whether and how they should engage in the different processes. For countries like Ireland that are strong EU members and committed UN member States, such options for international engagement are important.

On defence: geopolitical developments have made maritime security and the protection of critical undersea infrastructure a priority topic in the European context. Defence forces and their navies are reviewing and adapting their strategic defense and maritime security doctrine and policies to attend to new threats in the maritime domain. Some countries are developing seabed warfare strategies, identifying how they can bring to bear different skillsets to deliver effects using both existing and new systems.

For countries like Ireland that have a maritime domain seven times its landmass and with a lot of diverse activity on and in its waters, having the right strategies, capabilities and domain awareness is key, as is participating in strategically important projects relevant to CUI protection within the EU and, where applicable, through its International Tailored Partnership Programme with NATO.

For many countries, what is missing is shared awareness and understanding between government agencies and industry of the threats and challenges at hand. Establishing cross-government liaison and coordination with agencies and industry actors within and across countries that have an interest in the maritime domain is important, not least given the conflicting demands on the maritime environment and the need for coherent marine spatial planning on the one hand, and coordinated maritime security, defence and deterrence policies on the other. Advances in data sharing to enhance maritime domain awareness, aided by leveraging new sensing technologies and AI, and establishing mechanisms for intelligence and data sharing will help strengthen both security and resilience. Symposia such as these which bring together key government agencies with industry to discuss challenges from a holistic rather than a siloed perspective is key to problem solving and should be a more regular occurrence. In short, cooperation is necessary and can take many forms. Mutual listening to experts builds trust, good policy, and situational awareness. Multinational and interdisciplinary work is also needed in academia.

Governments are particularly interested in the intelligence collection opportunities presented by DAS and other sensing technologies. However, there are concerns that such changes to the character of subsea cables – from a transmission infrastructure to a large-scale, capable sensor on the seafloor – could make them more legitimate military targets during armed confrontations. In addition, changing the nature of what the cable does, can also change the legal frameworks for permitting and consideration under international law, and could increase regulatory/permitting burdens, which already exist as a significant challenge for subsea cable resilience.

It is also possible for malicious state or non-state actors to target the subsea cable network without fully understanding the fallout from their actions. Government officials need to understand the potential cascading effects – whether significant or not – of downed cables on their national infrastructure. Additionally, from a national preparedness perspective, and for coordination with partners, it is important to clarify roles and responsibilities across defence, law enforcement, diplomacy and industry. It is also important to consider some of these issues from a societal resilience perspective, not just resilience of the infrastructure in and of itself.

Regardless of developments underway, there is still a big disconnect between stated national policy aims and direction, and the ability to respond with the right capabilities. There is also a disconnect between the materiality of the problem at sea and how increased attention to what is happening under the sea through different technological means can create incentives for hostile actors to interfere and force a knee-jerk political response. And as discussed in previous panels, there is also a disconnect between how governments attend to high-impact, low probability events such as sabotage (or the threat thereof) and how they attend to the lower-impact, high probability events that affect the industry on a daily basis. Both need to be addressed.

From an industry perspective, political interest in subsea cables ebbs and flows, and manifests differently across regions in accordance with context. On actual damage to cables in peacetime, all repairs are carried out in the same manner regardless of cause. Geographically diverse redundancy providing rapid rerouting of data traffic, as well as the timely repair of damaged cables can also render sabotage less effective and thus serve as a deterrent. Repairs must be completed in as timely a fashion as possible, including in geopolitically tense areas. As evidenced in the Red Sea, this becomes more complicated under live fire, and a range of complex legal issues in addition to potential loss of life have to be considered.

It has happened that an ordinary repair operation at sea can find itself in the middle of a stand-off between countries' navies or coast guards, but in general the industry does not feel threatened and can get on with its operations. Being aware of all eventualities and knowing when to call on the support of a given navy or coastguard for a repair operation is important. For now, however, where geopolitical tensions are most felt is through permitting for installation and repairs, in that governments can use permitting requirements to purposefully delay permit granting for new systems or repair activity. Subsea cables cross multiple jurisdictions including disputed waters and geopolitical hot spots; hence the issue is a long-standing consideration for the industry in route planning and design.

Lastly, there is a maritime skills deficit not limited to the subsea cable industry. It is evident across government and academia. Low profit margins have made it difficult for maintenance providers to outcompete other industries and entice experienced operators and young trainees alike to join repair fleets. Cable maintenance must become an attractive industry for workers to join.

Panel 4

Fault Prevention and Cable Repair Ecosystem

The fourth panel explored the diverse challenges for subsea cable fault prevention and the measures necessary to ensure timely repairs.

Key Takeaways

- Threats to subsea cables vary significantly across regions. Systematic collection of baseline data helps identify trends, which in turn informs industry plans and government policy and regulation.
- Greater harmonization and alignment of regulatory frameworks, permitting regimes, and cable charting practices is critical to subsea cable resilience. Some countries also need to update their regulations specific to cable damage and penalties and ensure proper enforcement.
- Effective collaboration among stakeholders, investment in maintenance and repair capabilities, and improved communication with other seabed users are critical to enhancing cable fault prevention and timely repairs.
- There is a need to clarify roles and responsibilities across government and industry in heightened security contexts. While industry is already confronted with situations such as having to interact with an internationally sanctioned actor after the 2024 Red Sea incidents and an increase in suspected cases of sabotage of the infrastructure they own or operate, ensuring security in such contexts is the prerogative of governments.
- Questions of sovereignty and jurisdiction can complicate repair operations, particularly in situations of crisis and conflict. Regular public-private engagement can contribute to problem solving.

Main Discussion Points

Threats to cables vary very much by region, influenced by factors such as human activity and natural hazards such as seismic events. As fishing and anchoring remain the primary global causes of cable damage statistically, any meaningful fault prevention in peacetime necessitates effective collaboration between marine industries and between industry and governments. Seismic risks, while less common statistically on a global level, present the highest risk in certain regions, which emphasizes the need for context-specific approaches to cable protection. For example, commercial fishing is generally not the cause of cable faults in Japanese waters. Rather, the primary cause of damage in Japan is seismic events. In contrast, in the waters off the UK, the main cause of cable faults is commercial fishing. In both contexts, trends in data faults inform regulatory actions that allow for expedited repair.

Scenarios of multiple outages raise particular resilience issues. Whether due to natural events such as underwater landslides or sabotage, there is limited slack in the system with a limited number of vessels stationed around the world. Therefore, when multiple outages occur, it can take a longer time to repair. Shortages in cable spares, jointing kits, equipment, skilled personnel, and repair vessels exacerbate the challenges of responding to simultaneous incidents. However, as is, these challenges are well managed by the industry and the cable repair ecosystem functions effectively despite the known challenges. Nonetheless, new forms of public-private engagement are helping identify how to overcome potential shortfalls, including for those countries or regions that may experience significant delays in repair times, and on how the repair eco-system would deal with multiple breaks in a less cooperative international environment.

Effective and predictable regulatory frameworks were highlighted as key to ensuring cable resilience. Key factors include updating and enforcing cable damage legislation, easing cabotage and import licenses, ensuring that permitting processes do not impede repair commencement, being aware of industry norms and good practices and their geographical specificities, and understanding where measures such as cable corridors or cable protection zones may or may not be effective. There is potential for standardisation of permitting and other regulatory measures, especially across connected countries. However, there are mixed views on the prospects of achieving harmonisation at the global level.

Route engineering practices over the years have contributed to ensuring that cables are laid along the safest and most viable routes. Industry players have voiced serious concerns that greater government intervention in cable routing (e.g., for security purposes, or due to legislative barriers or jurisdictional creep) may undermine resilience. Engagement with relevant industry bodies such as the ICPC and ESCA, and operators in the development of marine spatial planning is therefore critical.

Repair operations for damaged cables rely on experienced personnel to operate ships, handle subsea cables, undertake specialised jointing and other roles, each requiring specific skills and expertise. While the industry demonstrates strong general collaboration through maintenance zones and private repair agreements, significant workforce and capability challenges remain. Resolving these requires long-term investments in attracting new talent to the workforce, dedicated training of cable engineers and specialist personnel; investing in the aging repair fleet and resolving the limited availability of repair vessels; and ensuring that sufficient spare cable and jointing kits are available in the relevant storage locations. Additionally, learning from incidents and repair operations help identify where additional protection measures are required. The panel emphasized the importance of these topics for the industry to ensure system resilience. For governments, awareness of these issues and challenges and how their own actions, be they regulatory or otherwise, can contribute to mitigating them is key for national preparedness. Simply investing in sovereign repair ships or pulling ships out of their maintenance contracts may not necessarily solve the issues.

Countries like France, the USA, and China are investing heavily in the subsea infrastructure eco-system, which encompasses repair capabilities and land-based networks. Panellists debated how such investments could shape the global repair and maintenance ecosystem, as well as their potential geopolitical implications.

Engagement with fisheries and other seabed users is vital to reducing cable incidents. Strong communication, accurate cable charting, and the use of collaborative maritime safety projects such as KIS-ORCA and the Kingfisher hazard bulletin ensure that stakeholders are aware of cable locations, which supports safety of life at sea to prevent snagging incidents, and in turn helps prevent damage and establishes clear liability as the cable owner has taken appropriate measures to publish the location of their seabed infrastructure and disseminate it to other sea users. This can support the ascertaining of liability when incidents occur.

There are specific obligations on asset owners to provide compensation for gear that has been sacrificed by fishers to avoid damaging a subsea cable – or potentially having a loss of life incident. KIS-ORCA and cable awareness charts provide emergency contact details to facilitate dialogue during an incident between fishers, the Coastguard, and cable owners.

Transparency and collaboration foster better "good neighbour" relations and reduces risks in shared marine spaces. Government enforcement of mandatory AIS can also help prevent cable damage to support vessel monitoring and tracking, while ensuring timely access to VMS data can help to ascertain cause of damage.

In scenarios involving broader security threats or live conflicts, governments play a critical role, even if the systems are owned and operated by private companies. Lessons from the Red Sea incident and the more recent Baltic Sea incidents where governments and industry have shared information point to a need to ensure effective crisis management and communications. Engagement between industry and government can also support repair activities to provide security in the event of a heightened risk to civilian vessels – or to expedite permits.

Take the incident in the Red Sea, where the stricken vessel RubyMar was abandoned with the anchor deployed which subsequently severed three cables. The repair activities were complicated by issues such as sanctions against the controlling party in the affected waters, which only the governments that had issued the sanctions had the power to resolve. As with other areas, these and other issues relating to state sovereignty and control will have a bearing over cable repair operations in the coming years.

Panel 5

The contribution of technology to cable security and resilience

The Panel discussed the role of technology in subsea cable security and resilience, focusing particularly on DAS. Discussions also centred on legal and regulatory issues emerging around the use of these technologies and the roles and responsibilities of government and industry when applying technology for undersea protection purposes.

Key Takeaways

- Sensing technologies such as Distributed Acoustic Sensing (DAS), State of Polarization (SoP), and bespoke sensors have advanced significantly. They have applications like environmental monitoring, disaster early warning, and situational awareness. Leveraging existing infrastructure, DAS allows real-time monitoring.
- Many governments are already using sensing technologies such as DAS for ocean observation, and early warning systems and are increasingly interested in their contribution to critical infrastructure protection. Effective situational awareness relies on combining data from multiple sensing technologies with inputs from AIS, VMS, radar, satellite imagery, and unmanned undersea vehicles. Machine learning offers significant potential to improve analysis and detect activity patterns.
- In one case where DAS use is required for monitoring for security purposes, the government of the relevant country has assumed the costs for installing the equipment.
- Other potential uses of DAS include confirmation/enforcement of AIS compliance and monitoring, as a means to prevent damage from fishing and other commercial activities.
- While DAS will not prevent cable damage from occurring from natural causes or human activity, including sabotage, its capacity to monitor in real-time can serve as an early warning tool and could be a deterrent. The range of DAS is currently limited to the first repeater (optical amplifier), and its use for purposes other than monitoring the cable itself faces unresolved issues under international law. UNCLOS has provisions relating to subsea cables that allow for scientific research so long as it does not exploit or explore the seabed in the EEZ. Other sovereignty and jurisdictional issues are likely to emerge.
- As DAS and other sensing technologies become more prevalent, there will be increased scrutiny on how and where data is managed and stored. Collaboration between governments and industry is crucial to address these challenges.
- Governments are prioritizing investments in undersea capabilities. Naval exercises and tabletop simulations help test operational concepts and decision-making processes.
- Mutual learning and cooperation across industries are vital for advancing subsea cable protection. Cooperation with other major marine industries that have undersea infrastructure is key, and lessons can be drawn from how they have used different technologies to monitor their own assets. An example of such cooperation is the Seabed User and Developer Group in the UK.

Main Discussion Points

Using a cable to take measurements undersea has a long history, dating back to the late nineteenth century when John Murray used electrical resistance measures along one of the first transatlantic cables. By analysing the differences observed, he made the first ever measurements of seafloor temperatures. Decades later, Henry Stommel used submarine cables off Florida to measure seasonal voltage fluctuations. These fluctuations showed, for the first time, a deep-sea current in the region - one of the key drivers of North Atlantic circulation and a critical factor in understanding the ocean's response to climate change. In short, cable-based sensing has significantly advanced our understanding of the ocean.

The sensing technologies available today include Distributed Acoustic Sensing (DAS), State of Polarization (SoP), interferometry and Optical Frequency Domain Reflectometry (OFDR). These fibre sensing technologies use the fibres themselves as a sensor and are therefore different to Science Monitoring and Reliable Telecommunications (SMART) cables which deploy bespoke sensors to gather environmental data. These are all different technologies or processes that measure different things with varying levels of sensitivity in that they have different ranges and spatial resolution. The technologies have different pros and cons depending on range, capability, cost, ability to retrofit, etc. The panel discussed their potential for contributing to environmental monitoring, to act as early warning tools for disaster management, and for enhancing situational awareness – but noted the legal challenges associated with them. They are seldom used in isolation. For instance, for situational awareness, it is the combination of data derived from some of these sensing technologies, as well as from other monitoring tools such as AIS, VMS data, radar and satellite imagery and data derived from manned and unmanned undersea vehicles, that can provide a relatively reliable picture of what is happening under the ocean and close to critical infrastructure. Machine learning provides an opportunity to improve this analysis and identify patterns of activity.

DAS has advanced very quickly in recent years. Since the fibre itself is the sensor, it is not necessary to install any additional equipment on the submersed part of the cable system and existing infrastructure can be used to do live measurements. If a user knows how to filter and process the data properly, they can have a real-time view of what is happening around the cable with very high reliability. Regular use can also help detect when vessels have turned down, or off, required monitoring systems such as AIS. It is also possible to filter out data so only data necessary to a particular output is collected. For example, data can be filtered to characterize shallow sediments or to identify the location of small earthquakes, processes which are key to informing decisions regarding cable burial or infrastructure construction on the seafloor. DAS has limitations in terms of how far it can extend (currently limited to the first repeater) although this technology continues to develop. Lastly, DAS is not a preventive tool - it cannot prevent damage caused by a natural disaster, anchor drag, trawling or the actions of a hostile actor. It can, however, provide greater awareness of the immediate activities taking place around a cable and support building a picture of maritime awareness.

The subsea cable industry's own research using DAS has produced important discoveries, for instance in relation to seabed flows or turbidity currents, and monitoring of seismic activity. Such discoveries, in turn, are important for informing cable route engineering decisions by both industry and governments, in order to ensure that cables are optimally routed to avoid known or anticipated hazards, where possible.

Governments are evidently drawn to this kind of capability. Already many are supporting the deployment of DAS and other sensing technologies for ocean observation and early warning for natural disasters. Sensing technologies could also be used as a deterrent against damage to cables caused by commercial fishing and other maritime activity and contribute to maritime monitoring and enforcement.

As the technology continues to develop and national security concerns increase, many governments will be keen to explore its use for infrastructure protection and to inform defence and national preparedness. While often raised as a risk, opinions differ on whether adding sensing equipment to a cable or by using the fibre itself as a sensor or by placing a sensor on cable equipment increases the systems' vulnerability to intentional damage. While such uses may elevate risk, they could also help mitigate it. The drive to collect data using DAS may prompt new regulatory requirements and scrutiny of how and where the data is managed, stored and protected. This could pose a risk to cable deployment and timely repair – therefore potential unintended consequences need to be fully explored. There are already important use cases of governments encouraging companies to use DAS to monitor critical infrastructure in their territorial waters and EEZ. In such cases, the government has assumed the additional costs of installing the necessary equipment. Distilling lessons from these and other such examples will be important for both government and industry moving forward.

Importantly, the use of DAS for purposes other than monitoring cable integrity and cable health remains unresolved under international law and is already becoming entwined in age-old issues of state sovereignty and jurisdiction, with some countries requiring prior consent for any data gathering that is done within its EEZ or on its continental shelf. It is possible to limit DAS, allowing only certain sections of the cable to be used to take measurements from each landing, which may assist with government confidence not to exert excessive regulatory burden.

From a defence perspective, governments are investing significant resources in undersea capability development, research and innovation, and clarifying priorities for future investment in these areas. This includes identifying how sensing and other technologies can be integrated into undersea infrastructure protection efforts. Such planning and prioritisation provide a basis against which relevant projects and initiatives can be evaluated. Making sense of the surface and subsurface data being produced through the different capabilities that are being deployed remains a key challenge. Naval exercises are particularly useful for verifying concepts of operations where Critical Undersea Infrastructure (CUI) is concerned, although these can be expensive to run. Tabletop exercises are an inexpensive alternative and help test decision-making and administrative procedures and identify challenges. Ensuring that relevant expertise, including from industry, is involved in designing and implementing these exercises can save a lot of time.

Lastly, as with other panels, mutual learning and cooperation is crucial for advancing subsea cable protection. This can include engaging with other sectors that have undersea infrastructure and drawing lessons from how they have used different technologies to monitor their own assets. One important difference between subsea cables and other critical maritime infrastructure is that much of oil and gas infrastructure is still State or semi-State owned and therefore benefits from additional protections and resources.

Roundtable 2

Subsea Telecommunications Cable Policy and Regulation for the Future

This second RoundTable focused on questions of regulatory certainty, as well as issues of coordination and protection in an increasingly crowded maritime environment with competing government priorities and industries.

Key Takeaways

- A greater number of activities are now taking place in the oceans, including subsea telecommunications cables operations, fishing, deep seabed mining, oil and gas, and offshore wind to name a few.
- Designating single points of contact, strengthening regulatory certainty, promoting the rule of law, and fostering information-sharing between these different industries and governments are essential for mitigating risks to subsea cables and other seabed users.
- The growing "spatial squeeze" in the oceans, with competing demands from a multitude of sectors with different priorities and policy mechanisms, will require innovative approaches to marine spatial planning. Greater coordination efforts between regulators, investors and operators are essential, as is learning from and coordinating with different countries' approaches to marine spatial planning.
- In the context of increasing seabed development, linear cables (telecommunications cables, interconnectors) require a route rather than a footprint and cross international maritime boundaries. Therefore, they have unique requirements when compared to other sectoral marine developments.
- Transparent, predictable and efficient regulatory processes (without jurisdictional creep) to facilitate the installation, operation and repairs of subsea cables is critical to the success of the industry.
- Despite the growing number of instruments and institutional arrangements established to protect subsea telecommunications cables and other undersea infrastructure, many of these instruments are not implemented or utilised to their fullest extent. Greater emphasis on the enforcement of existing regulations and greater harmonisation between existing instruments should be the focus of regulators

Main Discussion Points

Subsea telecommunications cables are subject to various risks and threats, including breakages caused by human activities (fishing, anchoring, dredging etc.), natural events, cyberattacks on network management systems or intentional breakages by malign actors. An increasingly crowded marine environment also poses risks, not just to subsea cables but to all industries operating in the maritime domain.

These and other risks can be mitigated through greater regulatory certainty and predictability, awareness of the importance of submarine cables, of environmental characteristics of cables, and of the sources of risks and threats to cables and historical efforts to mitigate them. Information sharing, too, is important but it needs to happen with other marine industries, between industry and governments, and within governments themselves to address stove piping and related problems. Designating single points of contact can help facilitate such information sharing. Continued promotion of the rule of law for the oceans, particularly the law of the sea convention (UNCLOS), not just ratification, but fundamentally the implementation of the provisions of that treaty can also address some of these issues. While industry plays a key role in some of these areas, and government in others, many are areas of shared responsibility and interest at national, regional and multi-lateral levels. Engagement and collaboration between government and industry, including through organisations such as the ICPC is optimum to achieving best practice.

Marine spatial planning is becoming an increasingly hot topic. The current 'spatial squeeze' in maritime jurisdictions, with telecommunications cable operations, fishing, deep-sea mining and offshore wind generation all vying for space and access is expected to increase in the coming years. Governments are focusing their attention on how to best manage that spatial squeeze in their waters and on the seabed. In this regard, clear and streamlined regulatory frameworks and processes (which are supported with input and technical expertise from industry to ensure feasibility) can help ensure that an operator's investments in the country's waters and on the seabed are appropriately balanced with a state's obligations are concerned, for instance, with respect to environmental protections.

Certainty, predictability, and clarity could be facilitated by the creation of 'one-stop shops' and by designating a point of contact for subsea cable policy whereby as much is done as possible by a single government agency.

In Ireland, the newly established Maritime Area Regulatory Authority (MARA) was created to provide greater certainty for operators or investors, and to simplify the country's existing licensing regime. The Authority serves as a single point of contact for deciding on who does what and where in Irish waters. It provides any developer who meets the criteria with the right to occupy a certain part of the seabed. The new Maritime Area Planning Act (MAPA) extends the government's oversight out to the EEZ limit. Challenges have emerged since the adoption of this legislation, notably regarding how regulation is extended to the EEZ, but workarounds are being sought. Meanwhile a new Planning Commission has been established to serve as the main authorisation body for new developments, while MARA is the main enforcement agency for the maritime space. However, since multiple agencies are involved, a dedicated regulatory coordination structure is currently being established. There is also an ambition to create a centralised database for the authorisation of maritime activities, which could play a role in collating information and providing a better understanding of each sectors' planned activities.

Other positive examples of effective marine spatial planning discussed include the UK Crown Estate's Whole-of-Seabed approach to form a Marine Delivery Routemap in order to map seabed usage up to 2050 and to identify resilience challenges. The Crown Estate in England, Wales & Northern Ireland also facilitates relations and problem solving between seabed users. These and other such examples could potentially serve as models or for exchanges with other jurisdictions.

For industry, open dialogue and constant communication with licensing authorities and other departments that ultimately feed into a licensing authorities' decisions can help minimise costly surprises, including the potential transitional effects of new regulations. That kind of collaboration should extend beyond national level to support collaboration between those jurisdictions on each end of the cable to ensure greater harmonisation of rules. It should also cover repair and recovery, not just laying of cables. The European Union's recent Recommendation on Secure and Resilient Submarine Cable Infrastructure was cited as an important development in terms of its drive to streamline regulation across the region, promote existing frameworks to find solutions to regulatory challenges and reduce burdens, map the existing cable landscape to identify resilience gaps and examine repair and recovery issues.

Government and industry actions ought to be complimentary to one another. A specific obstacle which was identified was potentially posed by incoming legislative changes. If new regulations such as NIS2 result in the creation of new agencies or the transfer of regulatory powers, knowledge or expertise could be lost in this process which could in turn obstruct collaboration between government and industry.

Asked if there was a risk that closer engagement between regulators and industry could result in conflicts of interest, panellists concluded that there is limited likelihood of that occurring if regulators understand the industry they are regulating, and if industry understands that regulators are focused on their primary objective of preventing harm and cannot give preferential treatment to any one industry or operator. Sufficient guardrails should be in place to prevent conflicts of interest and buffer against risks that might emerge from greater collaboration and information sharing.

ANNEX 1: Symposium Agenda

Inaugural Symposium on Subsea Cable Security and Resilience
10-12 October 2024

Valentia Island Transatlantic Cable Station, Valentia Island, Co. Kerry, Ireland

DAY 1 - Thursday 10 October '24

LAUNCH DAY - [Hybrid: in-person and online]

A Call for Presentations (CfP) was issued in early 2024 with the aim of attracting innovative and diverse thinking on security and resilience of subsea telecommunications cables. The first day of the Symposium showcased the selected abstracts and served as an important segue into the following 2 days of proceedings.

TIME	TOPIC	LOCATION
11:30 -12:30	Registration	*The Cable Station*
12:30-13:00	**Opening and Welcome** **Key Note** *The Valentia Island Cable Station and its History*	*The Cable Station*
13:00-14:15	**History, security and geopolitics** (*CfP stream 1)* - *From French fishermen to Russian submarines: 174 years of subsea cable security* - *Cable Protection in Cold War Strategic Thinking* - *Australia's Seabed Lines of Communications* - *Subsea Cable Security in the Pacific: Effects and Implications from US-China Digital and Technological Competition*	*The Cable Station*
14:15 - 14:30	*Break*	
14:30 - 16:00	Perspectives on Protection and Resilience (*CfP stream 2)* - *Sabre rattling or strategic resilience? Building better outcomes through informed policymaking* - *Resilience Unlimited* - *Enhancing Subsea Cable Resilience in the Caribbean* - *Responding to threats to undersea cables: Ireland's options as an EU member state* - *Exploring Alternate Bases of Jurisdiction under International Law for Submarine Cable Protection* - *Sabre rattling or strategic resilience? Building better outcomes through informed policymaking*	*The Cable Station*

TIME	TOPIC	LOCATION
16:00 - 16:15	*Break*	
16:15 - 17:15	**Technology, Security and Resilience** (CfP stream 3) - *Technical aspects of subsea cables for resilience* - *An AI-based approach to protecting critical underwater infrastructure: Project VIGIMARE* - *Subsea Cable Security Through Enhanced Monitoring* - *Public-Private Collaboration to Protect Critical Information Infrastructure in Ghana*	*The Cable Station*
18:00 - 18:45	**Origins - The Transatlantic Connection** *Live Demonstration of Connection between Valentia Island and Hearts Content cable stations*	*The Cable Station*
19:30 - 21:00	**Symposium Welcome Reception** *Keynote address, "A Momentary Sense of Wonder: A Message from the Transatlantic Telegraph of 1858"*	*St. John the Baptist Church*

DAY 2 - Friday 11 October '24

TIME	TOPIC	LOCATION
09:00	**Welcome** **Keynote Address by Tánaiste Micheál Martin, TD**	*The Cable Station*
9.30 – 11:00	**Panel 1: Subsea Cable Security and Resilience: Learning from the Past**	*The Cable Station*
11:00-11.15	*Break*	
11.15 – 12.45	**Panel 2: The Present: Getting subsea cable security and resilience to meet**	*The Cable Station*
12.45 – 13.45	*Lunch*	
13:45 - 15:15	**Panel 3: Subsea cable incidents: Current policy and practice**	*The Cable Station*
15.15 – 15.45	*Break*	
15.45 – 17.15	**Roundtable 1- Operating in a Heightened Geopolitical Context**	*The Cable Station*
17.15-17.30	**Wrap up Day 1**	
19:00-19:45	**Pre-dinner Fibreside Chat** The China Question: Navigating interests and narratives	*The Royal Hotel*
19:45 -20:30	**Symposium Dinner**	

DAY 3 - Saturday 12 October '24

TIME	TOPIC	LOCATION
08:30	**Arrivals**	*The Cable Station*
09:15-09:30	**Opening/ Welcome Day**	*The Cable Station*
09:30 – 11:00	**Panel 4: Fault Prevention and Cable Repair Ecosystem**	*The Cable Station*
11:00-11:30	*Break*	
11:30 – 13:00	**Panel 5: The contribution of technology to cable security and resilience**	*The Cable Station*
13:00 – 14:00	*Lunch*	
14.00 – 15.30	**Roundtable 2: Subsea Telecommunications Cable Policy and Regulation for the Future**	*The Cable Station*
15:30 – 16:00	**Wrap up with final reflections from panel chairs/moderators**	*The Cable Station*
16:00	**Symposium Closing**	*The Cable Station/ The Royal Hotel*

Notes