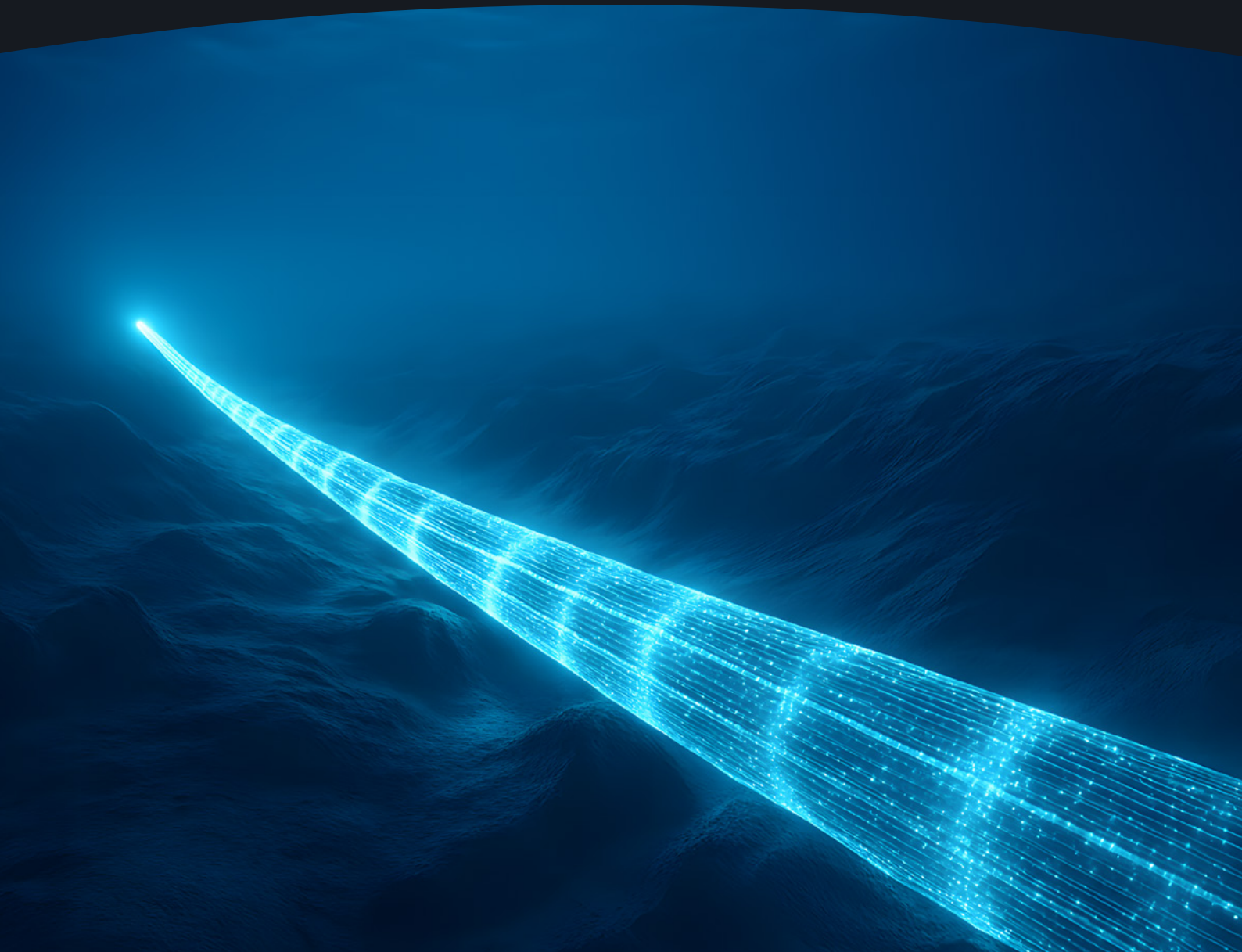
UNIDIR

Achieving Depth

Subsea Telecommunications Cables as Critical Infrastructure

CAMINO KAVANAGH • JONAS FRANKEN • WENTING HE



Acknowledgements

Support from UNIDIR funders provides the foundation for all of the Institute's activities. This study was produced by UNIDIR's Security and Technology Programme (SECTEC), which is supported by the Governments of Czechia, Germany, Italy, the Netherlands, Norway, the Republic of Korea and Switzerland, and by Microsoft. SECTEC's Cyber Workstream is also supported by the Governments of France and the Russian Federation. In addition, we extend our gratitude to the Department of Foreign Affairs of Ireland and the International Cable Protection Committee (ICPC) for providing additional support for this study.

The authors would like to express their appreciation to the government and industry representatives, as well as researchers, who contributed to this year-long research project. Special thanks also go to Paula Meissner, Franziska Schneider, and Julian Löffler for their assistance with proofreading, referencing, and graphic work.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

Citation

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

Cover Image: Generated with AI.

Authors

Dr. Camino Kavanagh

Research Fellow, UNIDIR Security and Technology Programme

Dr. Camino Kavanagh, the lead researcher on this report, is a Research Fellow with UNIDIR's Security and Technology Programme, and a Visiting Senior Fellow at the Department of War Studies at King's College London. She also works as an international consultant on issues pertaining to cybersecurity, critical infrastructure, international security and conflict. Among other roles, Camino served as Advisor/Rapporteur for the 2019–2021 Open-ended Working Group and Group of Governmental Experts on ICTs and International Security and for the 2016–2017 GGE on the same topic.

Jonas Franken

Research Associate, Science and Technology for Peace and Security

Jonas Franken is a Research Associate at the Science and Technology for Peace and Security (PEASEC) research group in the Department of Computer Science at the Technical University of Darmstadt and works on the project SecFOCI funded within the National Research Center for Applied Cybersecurity ATHENE. His research is located within the nexus of technology, policy, and international law, focusing on the resilience of critical communication infrastructures, as well as emerging issues in maritime security. He holds a bachelor's degree in politics and law and a master's degree in international studies / peace and conflict research from Goethe University Frankfurt and the Technical University of Darmstadt.

Wenting He

Associate Researcher, UNIDIR Security and Technology Programme

Wenting He is an Associate Researcher in the Security and Technology Programme at UNIDIR, where her work explores the intersection of international security and emerging technologies. She holds a master's degree in international affairs from the Graduate Institute of International and Development Studies, Geneva, and a bachelor's degree in diplomacy from China Foreign Affairs University, Beijing.

Acronyms & Abbreviations

CER	Critical Entities Resilience Directive (EU)
CI	critical infrastructure
EEZ	exclusive economic zone
ICPC	International Cable Protection Committee
ICT	information and communications technology
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NIS2	Network and Information Security Directive (EU)
UNCLOS	United Nations Convention on the Law of the Sea

Table of Contents

Executive Summary

This report is concerned with what it means in policy and practice when States designate or qualify subsea telecommunications cables as critical infrastructure. It aims to provide greater conceptual clarity to ongoing discussions by organizing observable government practice in terms of how it contributes to the resilience cycle, notably those **absorptive, restorative** and **adaptive** capacities a system requires to "anticipate, resist, absorb, respond to, and recover from negative impacts, carry out its original functions, and adapt in response to lessons learned from past experience or changed circumstances" (see figure 1 below). While the systems are generally designed and deployed with these capacities in mind, effective government action on security and resilience can contribute to strengthening them.

Government attention to the security and resilience of subsea telecommunications cables has intensified in recent years. While largely owned and operated by private companies, a growing number of States now qualify or designate the systems as critical, if not strategic infrastructure, the security and resilience of which are vital to economic and societal well-being, national security and much else. Under such a consideration, government efforts can be examined in terms of how they contribute to strengthening the systems' resilience capacities, and, by extension, societal resilience.

For now, most observable State practice falls under the **absorptive capacities** rubric. This makes sense since it is the stage in the resilience cycle that involves putting in place all the structures and mechanisms – the security and resilience scaffolding, so to speak – that play a preventive role or that enable action in the event that something happens. In this regard, some States are updating, streamlining or realigning their regulatory frameworks to reflect a heightened security context, while also attempting to ensure greater coordination with other policy and regulatory areas. Many are conducting consultations to identify potential barriers to investment for additional redundancy and for meeting capacity demands. Some are seeking to understand changes in cable ownership structures and relevant regulatory and national security implications. In some instances, a critical infrastructure qualification is helping to release budgetary resources to cover the costs of the personnel and the procurement, testing and deployment of new equipment and capabilities, particularly for maritime domain awareness and for informing defence and deterrence strategies. In light of the uptick in incidents at sea affecting undersea infrastructure, a number of States are integrating subsea cable security into their national preparedness and crisis response plans. This includes establishing coordination arrangements at different levels, designating points of contact at policy and operational levels, and reviewing mechanisms for engaging with industry, including to monitor and deter malicious activity. It also includes establishing new mechanisms to enhance situational awareness of threats to and vulnerabilities of the systems at sea, on land and in cyberspace.

From a **restorative capacity** perspective, regulation also matters, and some States and regional bodies are considering how to potentially ease permitting requirements or enhance cooperation to ensure more timely repairs. A growing number of States have launched public consultations or tenders to identify market failure and where government funding or investment may be needed to support

maintenance and repair. In some regions, new funding sources are being established to cover such gaps. Recent incidents and exercises are also testing how governments respond to incidents.

Where **adaptive capacities** are concerned, recent events and incidents are also providing useful insights to governments as they review their national resilience frameworks, maritime and cyber security strategies, and naval doctrine and operations. In many instances, learning from these incidents has prodded increased government investment in longer-term planning, knowledge development and awareness-raising, and a greater consideration of identified gaps in international law and how they can be addressed. Additionally, subsea cable security and resilience has become a topic of cooperation, within and beyond borders, marking a new era of cable diplomacy, so to speak. Beyond diplomatic action triggered by recent cable damage incidents, there are increasing exchanges within and across regions on national policy, regulation, national preparedness and crisis response relevant to subsea cable systems. Such exchanges also serve as a basis for enhancing dialogue and building trust across public and private sectors, essential to spurring a much-needed shift to more collaborative or integrated approaches to emergency planning and risk management, and the information- and intelligence-sharing required to enable it.

However, these and other efforts vary significantly across States in terms of their implementation and maturity. Indeed, the practical differences that occur as a result of a critical infrastructure designation vary significantly from country to country. There is limited conceptual clarity around subsea cable security and resilience objectives and capacities, driven in part by how the topic is considered by different policy communities, some which emphasize security more than resilience and vice versa. For some it is a telecommunications and capacity issue, tightly linked to economic prosperity, digital transformation, trade and competition. For others it is a cyber or supply chain security issue. Others approach it from a disaster preparedness and societal resilience perspective. And yet others from the perspective of maritime security or seabed warfare. In reality though, it is all of these and much more, making it a whole-of-government issue requiring whole-of-government coordination and a tight balancing of security and resilience measures.

Skills, capabilities and resources are an important challenge. The risk of government regulatory underreach or over-each is another, as is the risk of government underreaction or overreaction in the event of cable-related incidents. Here in particular, there is a need for greater alignment between security and resilience in national policy and response frameworks. The complexity of the regulatory environment merits particular attention, not least for the additional costs and burdens that new measures imply for both government and industry. And there is a pressing need for greater alignment between regulators and other government departments and agencies within and across the different jurisdictions where cable systems land. For many States, the shrinking subsea cable ecosystem brought about by new cable ownership structures raises a host of new regulatory and national security questions. And the absence of a long-term vision and approach to subsea cable policy and regulation can significantly impact digital transformation needs and objectives.

We argue that even in the current geopolitical context, sustained commitment and investment can contribute to addressing many of these challenges when the systems are considered as critical infrastructure. In this regard, we

suggest that the time is ripe for States, in collaboration with relevant industry partners, to:

- Develop and fine-tune their subsea cable security and resilience frameworks in accordance with their national context, ensuring they are attuned to evolving system architectures and a changing global environment. This effort should include setting clear objectives and measurable benchmarks. It should prioritize government actions that enhance the absorptive, restorative and adaptive resilience capacities of the systems and that contribute to overall societal resilience. It must also consider dependencies on the infrastructure and with other infrastructure and services, both within and beyond borders, and carefully balance equities with other policy areas. We summarize what such a security and resilience framework might look like in Table 1 below.
- Promote better understanding of faults and related effects, including how redundancy works to keep data flowing. This can help governments identify thresholds for reporting, categorize relevant incidents in terms of their scale and severity, confirm roles and responsibilities across government and industry for national preparedness and crisis response in peacetime, crisis and conflict and inform investment decisions in maintenance/repair capabilities. Particular attention should be given to strategic communications.
- Strengthen responses to cable damage at sea, including by:
  - updating relevant national law and regulations to ensure they appropriately reflect the criticality of the infrastructure;
  - identifying pathways for the adoption of new vessel standards and requirements, including for securing of anchors on vessels prior to passage and when underway; and
  - establishing cooperative mechanisms to protect against and respond to intentional damage of subsea cable systems.
- Increase exchanges of national views and practices in key areas such as:
  - streamlining licensing and permitting for installation and repair;
  - harmonizing regulation across connected countries;
  - innovation and investment in maintenance and repair;
  - subsea cable security and resilience in national preparedness and crisis response planning;
  - thresholds for incident and outage reporting and approaches to subsea cable incident classification;
  - handling cybersecurity vulnerabilities;
  - sensing and other technologies for early warning; and
  - addressing identified gaps and emerging issues in international law.
- Avail of new platforms such as the International Advisory Group led jointly by the International Telecommunication Union (ITU) and the International Cable Protection Committee (ICPC) to provide more examples from across the globe of current best practices for cable protection; and to identify new areas of emerging practice.

Finally, we note that there is currently no one place where reliable, publicly-available information on subsea cable-related policy, law and regulation and relevant research can be easily accessed. To enable more informed and coordinated interaction on subsea cable security and resilience matters, we therefore recommend that public and private actors jointly invest in developing such a platform. UNIDIR's Cyber Policy Portal (**https://cyberpolicyportal.org**) is a useful example in this regard.

TABLE 1.

Subsea cable security & resilience: A sample framework for governments

CROSS-CUTTING ISSUES	
International law: Charter of the United Nations, United Nations Convention on the Law of the Sea (UNCLOS), Geneva Conventions, customary international law, United Nations General Assembly resolutions, agreed norms of responsible State behaviour (cyber)	
Critical infrastructure consideration/designation: national policy/law	
Public–private engagement: policy, regulatory, operational	
Principles: predictability, reliability, transparency, accountability, security and safety.	
Equities management: public–private engagement; security vs. resilience; security vs. privacy; transparency vs. confidentiality; national sovereignty vs. international cooperation; competing policy areas (environmental/biodiversity protection, energy, fisheries, deep-sea mining, cultural/heritage protection)	
ABSORPTIVE CAPACITIES The ability of a system to withstand or absorb shocks without significant loss of function by ensuring robustness, redundancy and preventative measures. It includes measures that are "scenario-unspecific and that strengthen the general, overall ability of the system to withstand any disruptive event", thus ensuring stability.	▷ Domestic law and regulations streamlined and in place ▸ Permitting and licensing for installation and maintenance/repair ▸ Spatial separation ▸ Cable charting ▸ Cable damage ▸ Cybersecurity ▸ Supply chain security ▷ National preparedness/crisis management plans in place ▸ Roles and responsibilities (authorities/Rules of Engagement) clarified ▸ Point of Contacts appointed at policy, regulatory, operational levels ▸ Protocols and procedures established and regularly exercised at all levels (information-gathering/data-sharing (intra- and inter-government; government–industry); incident/outage reporting; system monitoring; law enforcement/military patrols) ▸ Cable, route diversity and alternative redundancy options identified

	▸ System security priorities, authorities and operational protocols identified (physical/cyber of front haul, cable landing stations, backhaul, data centres, points of presence, network operations centres and management systems, maintenance/repair fleet, personnel, supplies, supply depots, supply chains) ▸ National capability needs identified and addressed ▸ Personnel needs identified and addressed ▷ International cooperation ▸ Diplomatic processes/tools identified ▸ Transparency/cooperative/stability mechanisms established
RESTORATIVE CAPACITIES The capacity of a system to re-establish performance as quickly as possible after a disruptive event. It involves actions that are carried out to revert the effects of a disruption.	▷ Regulation and guidance (measures for expediting access to cable ships for repair; physical/cybersecurity of repair vessels and operations + spares depots, supply chain requirements) ▷ Engagement with industry on maintenance/repair needs ▷ Procurement/investment gaps for maintenance/repair capabilities, spares and supply chains identified and addressed ▷ Incident/crisis response plans, protocols and procedures ready to be activated ▷ Capabilities ready to be deployed ▷ Diplomatic tools ready to be activated
ADAPTIVE CAPACITIES The ability of a system to adjust, respond to changing conditions, and evolve after a disruption. It also means implementing changes to current practices or policies, and learning from disruptions, i.e., everything that is needed to improve before the next crisis.	▷ Learning from incidents and exercises and cross-sectoral collaborations ▷ Regular reviews of policy, law, regulation, standards ▷ Regular risk management reviews and application of post-review recommendations ▷ Diplomacy/international cooperation (long-term engagement): ▸ Subsea cable diplomacy toolbox developed ▸ Subsea cable security and resilience integrated into foreign policy engagement and diplomatic training ▸ Development/fine-tuning of transparency/cooperative/stability mechanisms ▸ Pathways for resolving existing challenges (e.g., vessel/anchor safety standards) identified ▸ Pathways for addressing gaps and emerging issues in international law identified ▸ Awareness-raising/capacity-building on regulatory best practices ▸ Awareness-raising/capacity-building on international law ▸ Financing for connectivity (beyond just the cable landing)

Submarine cable inspection vessel. Credit: Korn Srirawan / Shutterstock.

1. Introduction

In 1901, an international relations scholar warned of the societal, economic, and military and strategic significance of the submarine telegraphic service. Their disruption, he warned, would greatly disturb "the relations existing among the peoples of the world", as would any interposition of "the old barriers of space and time between the members of the human family". The economic activity of the world would be "even more disturbed" by any such interruption, since "it was originally for this field of the world's activity that the cable was laid". Shifting military and strategic tides in the decade leading to 1901 raised flags about policies of "construction [of submarine cables] on imperialistic instead of commercial grounds". And rising powers reciprocated by the institution of their own cable policies, bringing them under government control in times of peace and war.[1]

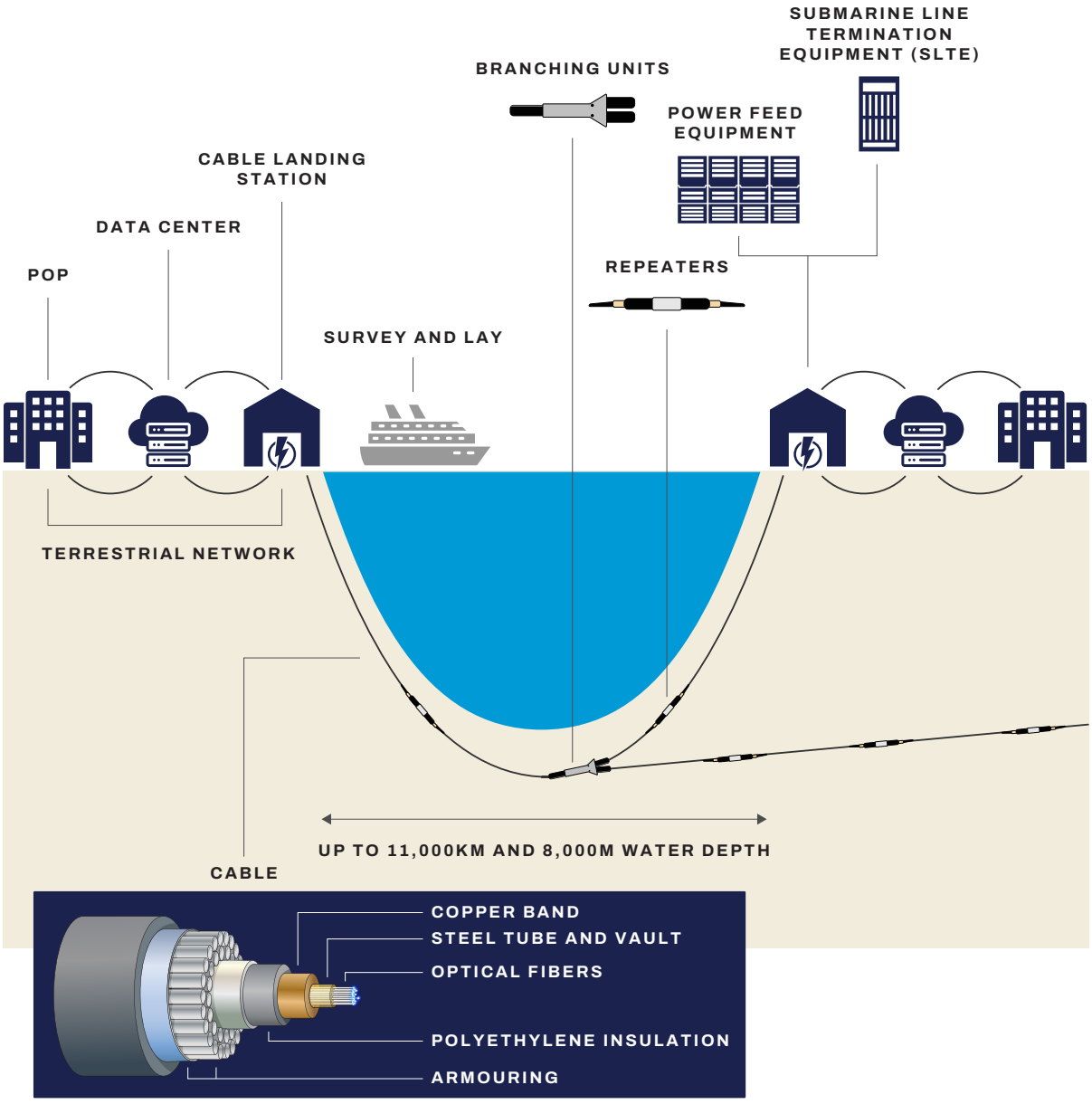
Today, submarine fibre-optic telecommunications cable systems (also referred to as subsea cables or subsea cable systems in this report, figure 1) are the backbone of our data and communications infrastructure, essential to the general functioning and integrity of the Internet and the broader information and communications technology (ICT) ecosystem. While satellites and the new constellations in low Earth orbit are breaking ground, especially in terms of lowering costs and accessibility, they are still no match to the high capacity and low latency that today's subsea cable systems provide. As more countries are connected, the security and resilience of the infrastructure becomes ever more critical. However, warnings similar to the ones issued in 1901 appear almost weekly in the media or in think tank reports. Governments and international organizations are paying attention, largely framing their approach to the topic as a critical infrastructure protection and resilience issue, meriting their intervention.

---

1 Wilson (1901), p. 6–11.

FIGURE 1.

Submarine Fibre-optic Telecommunications Cable Systems



In 2023 UNIDIR published a first report on subsea cables entitled "Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour".[2] Already, governments across the world were starting to pay attention to this infrastructure, notably its vulnerability – and by extension the vulnerability of societies – to a range of threats, including those involving malicious State actors. That report was a first scoping exercise, aimed at building awareness of this essential transmission technology, the industry at its heart, existing and emerging threats to the infrastructure at sea, on land and in cyberspace, how the infrastructure is governed, and how it can be made more resilient and secure. Since then, a slew of new initiatives has been proposed, including at the international level, to signal the strategic

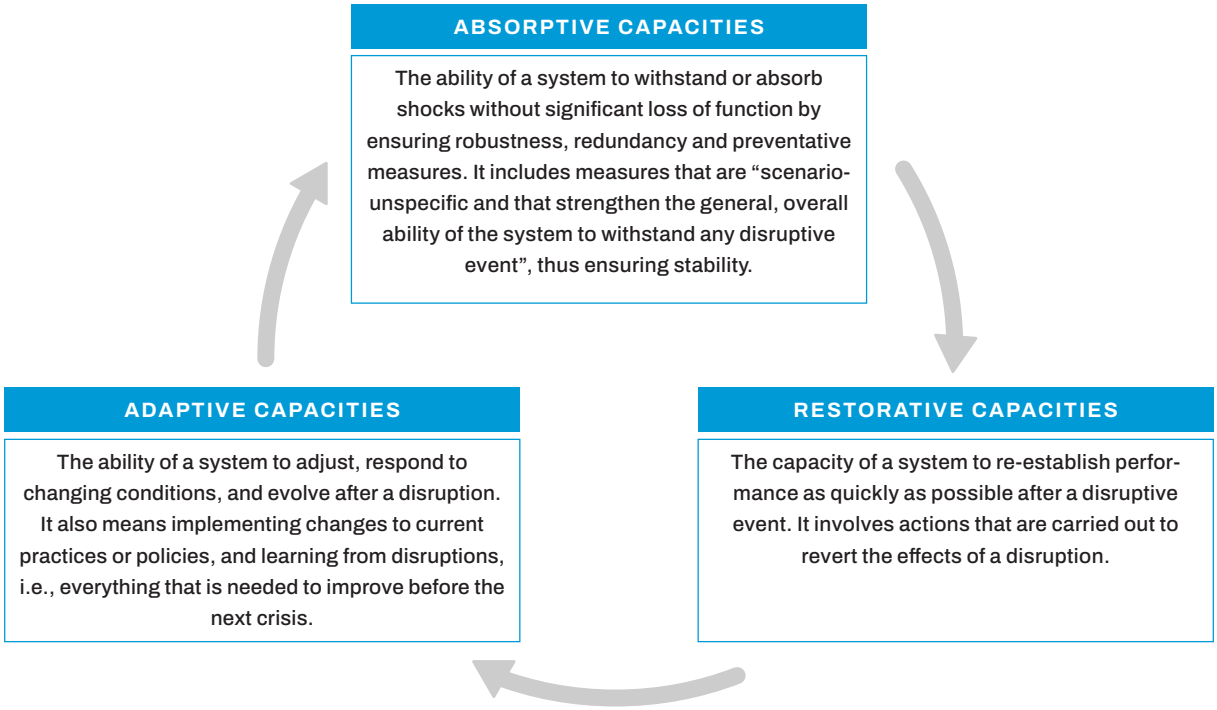
[2] Kavanagh (2023).

importance of the infrastructure, and the need to strengthen security and resilience across all of its components.

This follow-on study sets out to understand what it means in policy and practice when governments qualify or designate subsea telecommunications cables as critical infrastructure (CI). The report draws from the critical infrastructure literature to frame government approaches – proactive or reactive – to security and resilience, identifying how government policy and practice interacts with core CI concepts such as **absorptive, restorative** and **adaptive resilience capacities** (Figure 2).[3]

FIGURE 2.

Core Resilience Capacities: A Cycle



The report demonstrates that significant practice is emerging at national level, much of it consistent with recommended best practices and principles, and aimed at strengthening these resilience capacities. Yet, as we discuss, substantial challenges remain. Beyond a risk of regulatory over- or under-reach, practices differ considerably across States. There is a pressing need for greater alignment between regulators and other government departments and agencies within and across the different jurisdictions where cable systems land. There is also a need for greater alignment between security and resilience measures, and between subsea telecommunications policy and other key policy areas. Moreover, there is a need for greater conceptual clarity around subsea telecommunications cables when understood as CI. The resilience framework we propose is a first attempt to provide some conceptual clarity to government efforts. It breaks down such efforts into three overlapping capacities – absorptive, restorative and adaptive – which we view as fundamental features of the resilience cycle and as key drivers of societal resilience and national security.

[3] Elsner, Huck, and Marathe (2018).

A note on methodology

This report was developed on the basis of structured interviews with representatives from national governments, international and regional organizations, and industry. In identifying interviewees, we sought to ensure as much geographical representation as possible, although, as with many such projects, we were limited by time and resources. Desk research complemented the interviews. The report also benefited from feedback and insights garnered from a range of expert meetings and conferences held throughout 2024. Key among these was the UNIDIR workshop organized in the margins of the March 2024 session of the United Nations Open-ended Working Group on security of and in the use of information and communications technologies. Supported by the Government of Ireland and the International Cable Protection Committee (ICPC), the workshop served to present and discuss the parameters of the project. Other events that have been key to informing the report include the April 2024 ICPC Plenary held in Singapore and a follow-on regional expert meeting hosted by the National University of Singapore's Centre for International Law on the Law of the Seas and Submarine Cables; the September 2024 European Subsea Cables Association Plenary in the Faroe Islands, and the October 2024 Valentia Island Inaugural Symposium on Subsea Cable Security and Resilience.

A note on terminology

The terms 'submarine telecommunications cables', 'subsea telecommunications cables', 'subsea cables' and 'underwater cables' are used interchangeably throughout this report, reflecting the existing usage of the word 'submarine' in international treaties, and the growing usage of the word 'subsea' or 'underwater' cables alongside 'submarine cables' in national and international policy. Terms such as 'critical undersea infrastructure' refer to such cables as well as all other vital assets such as energy cables and pipelines.

Submarine cable laid on the seabed. Credit: anonymous.

2. Critical Infrastructure Protection: An Overview

There is a broad literature on the topic of critical infrastructure protection. It tends to be significant events – or a combination thereof – at national, regional or international level that serve as a catalyst for serious government intervention on the topic. The government policy roots of CI protection can be traced to the Cold War years, when fear of nuclear attack or other forms of sabotage pushed governments to strengthen the protection of key military and defence-related infrastructure and supply chains considered vital to national security. In the 1980s attention broadened to cover information security and other more technical systems, increasing in tandem with growing dependencies on ICT.[4] In the 1990s, the US government published the first policy documents on the topic, urging for the protection of both cyber and physical assets.[5] The focus on CI protection gained further traction following the terrorist attacks of 11 September 2001 in the United States, and attacks that followed elsewhere throughout the decade, leading to reassessments of approaches to CI protection, the establishment of new institutional arrangements at national level across States to lead such efforts, and the first national strategies and frameworks on the topic.

Globalization and the interconnectedness and interdependencies of economies and infrastructure in the 2000s brought to light the challenges of protecting increasingly digitized and networked infrastructure and services across borders. It also brought with it significant international collaboration and the development of global standards and practices for CI protection. Major events such as COVID-19 in the current decade placed emphasis on sector- or service-specific approaches, while natural hazards and climate change also inform approaches to CI protection, with resilience to events such as hurricanes, floods and earthquakes viewed as key elements of protection strategies and emergency planning.[6]

Today, CI protection has shifted from focusing merely on avoiding and preventing "unwanted events in certain CI sectors" and protecting specific assets to a focus on resilience and ensuring related system capacities.[7] As inter-State war has once again become a feature of international politics, in some regions there has been a shift in the treatment of CI. Key sectors and services upon which both civilian and military activities depend, such as communications, energy, transport, food and agriculture, and health and medicine, are now viewed at risk not just from commercial activity or natural hazards, but also from armed aggression by either State or State-backed actors, thus requiring a more integrated and comprehensive approach to resilience.[8]

---

4 Collier and Lakhoff (2008), p. 35.

5 In 1996, President Bill Clinton issued Executive Order 13010 establishing the President's Commission on Critical Infrastructure Protection.

6 Franken and Reuter (2024a).

7 Resilience capacities are directly associated with corresponding actions or processes – resilience is the ability to act resilient or "the capacity to execute the [resilience] processes". Pursiainen and Kytömaa (2023), p. 87; Mentges et al. (2023), p.2.

8 Niinistö (2024). Report by the former President of the Republic of Finland, in his capacity as Special Adviser to the President of the European Commission.

Within this broadening framework, resilience is largely understood not as static, but rather as "the ability of a system to deal with the impacts of unspecific and possibly unforeseen disruptive events". This ability depends on the availability and sophistication of a diverse set of skills and strategies, that is, the resilience capacities required to "anticipate, resist, absorb, respond to, and recover from negative impacts, carry out its original functions, and adapt in response to lessons learned from past experience or changed circumstances". In short, the concept integrates "the before, during, and after of an unwanted event or disruption, thus covering the whole crisis management cycle".[9] It ensures both stability and flexibility in the cyclic resilience process, with the ultimate goal of "strengthen[ing] the system capacities to better deal with future events, whatever form they might take".[10]

The capacities of the resilience cycle – and skills required to ensure them – are often referred to as '**absorptive**', '**restorative**' and '**adaptive**'.[11] **Absorptive capacities** refer to the ability of a system to withstand or absorb shocks without significant loss of function by ensuring robustness, redundancy and preventative measures. And in contrast to protection, "absorption measures are scenario-unspecific and strengthen the general, overall ability of the system to withstand any disruptive event", thus ensuring stability.[12] **Restorative capacities** in turn refer to the capacity of a system to re-establish performance as quickly as possible after a disruptive event. They involve actions that are carried out to revert the effects of a disruption, for example, sending out repair teams, repairing components by using spare parts, or ordering missing spare parts. Such capacities are enhanced by contingency plans, competent emergency operations, and the means to get the right people and resources to the right places.[13] For their part, the **adaptive capacities** of a system refer to the ability of a system to adjust, respond to changing conditions, and evolve after a disruption. Adaptive capacities also mean implementing changes to current practices or policies, and learning from disruptions, for example, through revising plans, modifying procedures, or introducing new tools, technologies, and training exercises – that is, everything that is needed to improve before the next crisis.

Private actors tend to own and operate most infrastructure today, and are generally guided by technical standards and best practices to ensure that systems are absorptive, restorative and adaptive. Governments, too, play a significant role.[14] For instance, governments contribute to ensuring CI **absorptive** and **restorative capacities** through regulation, risk management and mitigation measures, targeted funding or investments, and by putting in place emergency preparedness and crisis response arrangements, and the relevant protocols and procedures. Engagement and information-sharing with the private sector is key to each of these steps, and, depending on the infrastructure or service, may be required by law. Where **adaptive capacities** of CI systems are concerned, governments contribute through long-term policy and planning (e.g., resilience planning, or through incentivizing innovation), by ensuring that regulation remains flexible or adaptable to new challenges (even if this is not always the case); investing in

---

9 Pursiainen and Kytömaa (2023), p. 87; Hollick and Katzenbeisser (2024).

10 Mentges et al. (2023), p. 7.

11 Elsner, Huck, and Marathe (2018).

12 Mentges et al. (2023), p. 10.

13 Ibid., p. 11.

14 Pursiainen and Kytömaa (2023), p. 88.

knowledge-sharing, capacity-building and international cooperation; and through information-sharing and collaboration, particularly with the private sector and academia and across policy areas and sectors.

2.1. What is critical infrastructure and who decides?

The term critical infrastructure is a composite expression that draws its etymological roots from three elements. The prefix *infra*, originating from Latin, means 'below' or 'beneath', emphasizing the foundational and supportive nature of these elements in society's operations. 'Structure' pertains to the deliberate organization and construction of human-made systems. The term 'critical', derived from the Greek *kritikós*, signifies the capacity to discern, highlighting the pivotal importance of such infrastructure over others. Consequently, critical infrastructure broadly refers to indispensable systems and processes that are crucial for the functioning of a society. In practice, determining which infrastructure or services qualify as critical is the prerogative of individual governments, even if specific protections might be rendered through international law, or international, regional or specialized organizations. Given the ownership structures and complex supply chains of today's infrastructure, it is increasingly the case that private entities also play a significant role – at times, the lead role – in shaping how the infrastructure they own or operate is considered, although as we discuss later, this lead role often diminishes in tandem with heightened security threats, or perceptions thereof.

Nonetheless, there is general consensus that a criticality designation is tightly coupled with the functioning of society and the economy. Such a qualification would include assets, systems or services so vital that their unavailability or destruction would have a debilitating effect on national security, public health and safety, economic stability, or a combination of these. For instance, the **European Union** has shifted from an approach that focused merely on protecting specific CI facilities to one centred on protecting vital societal functions.[15] **China**'s 2021 Critical Information Infrastructure Security Protection Regulations covers "network infrastructure, information systems (...) in important industries and sectors the destruction, loss of functionality, or data leakage of which may gravely harm national security, the national economy and people's livelihood, or the public interest."[16] States of **Northern Europe** have long taken a societal approach to assessing criticalities. **Norway**, for instance, starts from the basis of those societal needs that are addressed by vital or critical societal functions. These functions, in turn, rely on infrastructures whose criticality is determined by factors such as reliability, availability of alternatives or redundancies and the degree of interdependency.[17] From there, a decision is made on whether an infrastructure is critical or not.[18]

Despite broad buy-in today to the need to ensure a balance of security and resilience in CI protection, getting these approaches to sync in national policy and practice is no easy task. First, in many instances there is often no consensus even within a given jurisdiction

---

15 The European Parliament (2022b) provides direction to member States on determining the relevant vital infrastructure and services.

16 Creemers, Sacks, and Webster (2021).

17 Pursiainen and Kytömaa (2023), p. 90.

18 Ibid.

over how to qualify a given infrastructure or service, which in turn creates legal, regulatory, policy and operational challenges. Second, the infrastructure and/or services delivered through the infrastructure may have national, cross-border as well as cross-domain elements, again creating legal, regulatory, policy and operational challenges. Third, developing and implementing strategies that account for the interconnected and interdependent nature of CI today, as well as their temporal and spatial spread, requires significant investment in time and resources by both private and public actors, often implemented through public–private partnerships or other such collaborative efforts. These efforts can carry significant burdens for all parties and are not easy to incentivize and implement in practice, often due to security and commercial reasons. Fourth, geopolitical factors undoubtedly drive concerns over the vulnerability of infrastructure systems and supply chains to new kinds of cyber–physical threats involving State actors (or proxies acting on their behalf), and the more direct involvement of defence, intelligence and economic security agencies in CI protection. These developments suggest a need to balance and align policy, strategy, operations, investments and incentives and stronger consideration of equities. Finally, an over-securitization of CI protection risks undermining the agency of other States and puts business and investment strategies at risk – and it can upend hard won rights such as privacy and data protection, particularly when appropriate checks and balances are not in place.

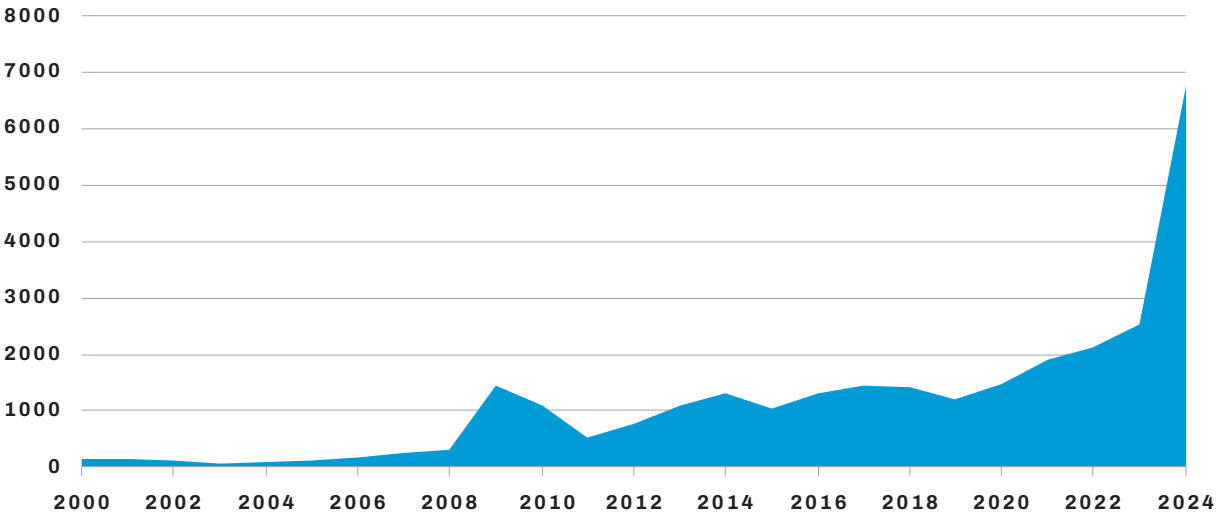
Submarine cable landing site. Credit: courtesy of Aqua Comms.

3. Subsea Cable Systems as Critical Infrastructure?

Despite all the attention to critical infrastructure protection in the 1990s and 2000s, until recently there was a general perception that subsea telecommunications cables were a "hidden infrastructure",[19] far from the mind of government decision makers and regulators. For instance, responses to the 11 September 2001 attacks covered large parts of the maritime sector, most importantly ports, through the International Code for the Security of Ships and of Port Facilities. However, subsea telecommunications cables and their landing stations were not affected by this first wave of CI protection, even if cable laying and maintenance fleets would have come under heightened security levels in ports. The level of attention afforded to the infrastructure is, however, highly dependent on context and dependencies. For some States, it has never been a hidden infrastructure, while for most others, it no longer is. As evident in figure 3 below, this shift is also reflected in media coverage of the systems.

FIGURE 3.

Co-occurrence of mentions of subsea cables and 'critical infrastructure' in news reports between 2004 (n = 103) and 2024 (n = 6,750).[20]



Submarine fibre-optic telecommunications cable systems are the backbone of global digital communication, transmitting over 99 per cent of intercontinental data. Currently, there are approximately 550 active submarine cable systems worldwide, with individual cables offering design capacities ranging from a few gigabytes per second to several hundred terabytes per second. These systems are engineered with a planned operational lifetime of 20 to 25 years, though their viability is tied to commercial demand. To ensure longevity,

---

19 Bueger and Liebetrau (2021), p. 391.

20 Figure by the authors. Data from LexisNexis news database with search terms 'critical infrastructure' in combination with 'underwater/undersea/subsea/submarine, data/internet, and cable/cables'.

cables are planned and built with significant overcapacity, which typically means they reach their maximum data throughput only in the final years of operation. This design strategy accommodates future growth in data demand and helps sustain their economic utility over decades.

States with the highest number of cable connections are the **United States**, **Japan** and **China**, while European States such as the **United Kingdom**, **France**, **Spain** and **Italy** lead in terms of numbers of cable landings in their territory. States close to a maritime choke point tend to be well-connected, as in the case of the **Republic of Korea** (Korea Strait), **United Arab Emirates** (Strait of Hormuz) and **Egypt** (Isthmus of Suez). Other choke points with a high density of cable infrastructures are Bab-el-Mandeb in the Red Sea, the English Channel, the Strait of Gibraltar, Strait of Florida and the Isthmus of Panama. In general, factors such as the presence of global financial centres, the economic wealth of a country, large and dense populations, technical infrastructures, as well as political and financial stability usually attract cable system construction.[21]

On the other side of the connectivity scale, only very few coastal territories remain completely disconnected from the global network: **Antarctica** is the last continent without any subsea data cable landing, although that may change some time soon. Two planned projects – one from **Chile** to **King George Island**[22] and another from **New Zealand** or **Australia** to the **US McMurdo Station**[23] – may change this situation in the coming years. **Eritrea** is the largest populated coastal country without any submarine connection.[24] More typically, small island territories like the **Pitcairn Islands**, the **Falkland Islands**, **Rapa Nui** or **Galapagos Islands** are not (yet) connected via a fiber-optic link, but must resort to lower bandwidth, high-latency satellite data transmission technologies for their international traffic. Also, numerous countries only have one international subsea cable link, which can lead to an situation of extreme dependency. Such countries – often small island developing States – are disproportionately impacted when cable damage occurs. Indeed, an outage of the single cable connection without a redundancy potential routing through another system usually leads to a large-scale blackout – especially when there is no meaningful satellite backup in place. The Pacific Island State of **Tonga** has experienced several such blackouts.[25] Other small island States and territories belong to this group and include **Kiribati**, **Niue**, **Cook Islands**, **Wallis and Futuna** and **Saint Helena**. Still, territories with redundant cable connections can be susceptible to outages, if multiple outages occur simultaneously or if rerouted traffic overwhelms the capacity of the redundancies. For example, this was the case in the Trou Sans Fond incident, in which an undersea landslide damaged multiple cable systems within hours and disrupted Internet services in multiple **Western African** countries in early 2024.[26] The consequences of such subsea cable outages can be significant,

---

21 Franken et al. (2025).

22 Multilateral Cooperation Center for Development Finance (n.d.). According to the publication 'Developing Telecoms', the Chilean regulator, SubTel, has received four different offers to carry out a feasibility study of a project to implement the first submarine fibre-optic cable between Chile and Antarctica. See Qui (2024). It has until January 2025 to deliver the results of the technical evaluation of the offers. Meanwhile, the US National Science Foundation also put out a 'Request for Information (RFI) relating to the Development of an Antarctic Subsea Telecommunications Cable for Science', 6 December 2024.

23 National Science Foundation (2022).

24 Franken et al. (2025).

25 Speidel (2022).

26 New York Times (2024).

affecting emergency and other essential public services. With many companies growing their Internet-dependency, not only in service-heavy economic sectors, but also in primary production like agriculture, mining and manufacturing, the economic losses of national or regional outages can be immense. Different redundancy options can mitigate these impacts, a point we return to later.

3.1. From 'Eureka moments' to normalization

Throughout history, commercial activity such as fishing and anchoring as well as natural hazards have been the principal cause of damage to subsea cables in peacetime. For instance, damage caused by trawling, the complexity of the maritime environment and the effects of natural hazards all featured strongly in the negotiations leading to the 1884 Convention for the Protection of Submarine Telegraph Cables and in negotiations around the cable-related provisions in the more recent 1982 United Nations Convention on the Law of the Sea (UNCLOS). At the same time, geopolitical considerations and the effects of wartime activity have been consistently in the background, also featuring strongly in the conferences leading up to the 1884 Convention, and in a number of different instruments adopted in subsequent decades. International focus on the infrastructure waned when satellite technologies supplanted subsea cables as the main means of inter-continental connectivity in the 1950s. It resurfaced in the run-up to UNCLOS negotiations, which preceded the massive expansion of intercontinental voice and data transmission enabled by the deployment of subsea fibre-optic cables and the Internet and prompting valid questions today as to whether the instrument's cable provisions remain fit for purpose. The current transition in the subsea telecommunications cable industry is happening at a time of significant global turmoil and questioning of the US-led global order that emerged at the end of the Cold War.

Subsea telecommunications cables are now intrinsic to the functioning of societies across the globe. The systems are generally designed and deployed in accordance with traditional engineering principles relevant to safety and resilience. The number of reported faults per annum has remained relatively steady despite the increase in the number of deployed cables, likely due to enhancements in cable protection such as route design and cable burial. It is common knowledge that the majority of damage to subsea cables still stems from fishing and other commercial activity as well as natural causes, with most faults occurring in water depths shallower than 200 metres.[27] However, this is not always what spurs States to build a case for considering subsea telecommunications infrastructure as critical and putting in place the necessary protections. Rather, it has tended to be major events that spur such attention. Indeed, there are situations – we refer to them as **Eureka moments** – that prod States to pay more attention to the systems and their potential vulnerabilities. These moments of insight are generally provoked by a single event. Suspected acts of terrorism or State-sponsored sabotage, which statistically are the least probable causes, often provoke the most significant response (as is the case today), although this is highly contextual and varies significantly across regions. Based on our research, the result of this attention is not always borne out immediately (or at all) in national policy, although as evidenced in Europe, this too is changing.

---

[27] Carter et al. (2009); Burdette (2024)

Consider the past couple of decades: For **Australia**, it was apparently a series of disruptions to subsea cable systems caused by anchor drag, trawling and dredging in the decade spanning 1991–2001 that drew attention to the vulnerability of the systems. It was, however, the heightened threat of terrorism in the early 2000s in addition to these incidents that propelled the 2005 legislative reforms and the foundations for Australia's somewhat robust, yet already dated, cable protection regime – generally viewed as the 'gold standard'.[28]

For **Algeria**, the 2003 Boumerdès earthquake, which generated a localized tsunami off the country's north coast, was an early wake-up call to the economic consequences of being disconnected from other countries, in this case from **France** and **Spain**. For key connectivity hubs such as **Singapore** and **Hong Kong**, their enduring attention to subsea cable resilience issues is linked to a 2006 earthquake which cut several cables simultaneously. The effects across the region motivated in-depth commissions of inquiry and reports at national and regional levels.[29]

For **China**, it was initially its own isolation and national economic development objectives that sparked government attention to – and massive investments in – both terrestrial and subsea telecommunications cables in the 1990s and 2000s, the period when its initial cable protection regulation was put in place.[30] This attention subsequently extended outwards, through global infrastructure projects, and with them, investments in manufacturing and other capabilities. Ever-souring relations with the **United States** on a wide range of issues, including on technology and telecommunications equipment writ large have catapulted subsea cables up the policy ladder in **both States**. Meanwhile, the effects of the 2006 earthquake in the region as well as the high frequency of cable faults in key maritime areas such as the **East China Sea** due to the intensive use of stow nets and pair trawling fixed attention on basic cable protection issues and law enforcement responses at home.[31] So too, have shipping incidents such as that which occurred in February 2023 in a maritime area near Shantou (north shore of the **South China Sea**) and which resulted in damage to four international fibre-optic cables, reportedly disrupting approximately 20 percent of the country's international communications.[32]

Countries across the world were affected by three major incidents in 2008. In the first, which occurred between 23 January and 4 February, some five cables were damaged, a "rare coincidence that (…) defied explanation".[33] In the second incident, which occurred late February, a cable between Singapore and Jakarta was damaged. In the third incident, which happened on 19 December, another four cables were cut. The effects of these incidents were widespread, hitting the **Middle East** and **India** particularly hard. While the cuts were determined to have been caused by bad weather, anchor abandonment, drop

---

28 Interviews, April–October 2024; The Parliament of the Commonwealth of Australia, House of Representatives (2005), p. 5–6.

29 APEC Policy Support Unit (2012), chp. 2, 'Dangers to and Disruptions of Submarine Cable Systems in the APEC region in 'Economic Disruptions to Submarine Cables'; Legislative Council Panel on Information Technology and Broadcasting Hong Kong (2007); Marle (2007).

30 State Council of the People's Republic of China (1989).

31 UltramapGlobal (2024).

32 Caixiong (2024); *The Nanfang Daily* (2024).

33 Allam (2008). The affected cables were SeaMeWe-4 near Penang, Malaysia, the FLAG Europe–Asia near Alexandria, FLAG near the Dubai coast, FALCON near Bandar Abbas in Iran and SeaMeWe-4, also near Alexandria; see Zain (2008).

or drag, speculation of State-backed sabotage was also high, not least since in one specific incident a ship underway dragged anchor for 300 km, severing several cables.[34] Such speculation quickly abated.

For **Japan** – a major cable hub – it was the 2011 tsunami off its southern coast and the ensuing damage to some nine international cables that laid bare its own connectivity vulnerabilities.[35] For **Tonga**, a small island developing State in the **Pacific** currently connected by just two international subsea cables, volcano blasts such as the one in 2019, and others that have since followed, clearly demonstrate the vulnerabilities of limited redundancy options.[36]

For **Egypt**, long affected by cable cuts off its coast, the arrest of three divers attempting to cut an undersea cable in 2013 off the coast of Alexandria, was yet another reminder of the potential vulnerabilities that come with its strategic location. The incident also had ripple effects on **United States** military operations overseas and led to the first public discussions in the United States on the cybersecurity of subsea cable systems.

In Latin America, **Brazil**'s consideration of subsea cables stems from a mix of factors: natural events and commercial activity, including on the other side of the Atlantic, that have caused disruptions to its systems, suspicious activity involving a certain naval power in its territorial waters and concerns about that State's espionage and surveillance practices and their potential impact on national security.[37]

Across **Africa**, it was the disruptions that occurred almost consecutively off the continent's east and west coasts in 2024 that most recently captured the attention of incumbent officials in both coastal and landlocked States.[38] **Nigeria** has since brought the issue to the international level, driving a new initiative within the International Telecommunication Union (ITU) to address subsea cable resilience issues. **Ghana**, in turn, has put in place new measures for subsea cable and mobile operators, and is also consulting with industry actors on specific recommended practices for cable protection in its territorial waters.[39] For the small island State **the Comoros**, the February 2024 Red Sea incident and subsequent disruptions off the African east coast have accelerated its efforts to attract new cable landings and to privatize the sector.[40]

For **Brazil, Ghana, India, Indonesia, Malaysia, Panama, Singapore, Thailand, Viet Nam** and **most other States** discussed herein, their attention to cables is tightly linked to their digital transformation and economic development ambitions, which can only be realized with the kind of connectivity that subsea cables provide, by mitigating some of the most common causes of damage, including fishing and anchoring, and by ensuring greater redundancy options. The latter is particularly pertinent for **Viet Nam**, which has had to manage multiple cable failures over the

---

34 Veverka (n.d.), p. 15; Hruska (2008); Murph (2008).

35 Kazama and Noda (2012); Cho et al. (2011).

36 Speidel (2022); Bricheno et al. (2024).

37 Interview and follow-up communications, April–October 2024; Agência Nacional de Telecomunicações Brasil (2023).

38 The West Africa cable outage of 13 March 2024 impacted Internet connectivity in 13 countries: Benin, Burkina Faso, Cameroon, Côte d'Ivoire, the Gambia, Ghana, Guinea, Liberia, Namibia, the Niger, Nigeria, South Africa, and Togo; see Internet Society (2024).

39 Inaugural Symposium on Subsea Cable Security and Resilience, Valentia Transatlantic Cable Foundation (2024).

40 Interview, February 2024.

past couple of years.[41] For **India**, the issue is also tied to the State's participation in new regional arrangements such as the Quadrilateral Security Dialogue, and its recent interest in investing in sovereign repair capabilities.

As for **Europe** and **North America**, memories of the effects of the **1929 earthquake** off the coast of **Newfoundland**, the ensuing turbidity currents of which snapped some 12 transatlantic submarine telegraph cables, have resurfaced in parallel with growing concerns about the security and resilience of the systems that today cross the strategic North Atlantic.[42] The recent uptick in attention to the systems is driven by the 2022 **Nord Stream pipeline blasts** and the series of **incidents previous to and that have since followed** in the **North Sea**, **the Atlantic**, **the Irish Sea** and **the Baltic Sea**, some of which boast strong hybrid undercurrents.[43] Lessons from – or the potential consequences of – such incidents are informing preparedness and crisis management and the consequent release of funds for more targeted maritime deterrence and defence initiatives between connected States, with industry and in specific maritime regions. In **Italy**, for instance, since 2022 the Navy collaborates with the country's largest cable provider to monitor and deter potential attacks on the infrastructure.[44] And as evidenced in the **Baltic Sea**, learning from the incidents is bolstering governments' response capacities, which in turn can helps bolster coordination, ensure timely investigations and inform attribution policies and future deterrence strategies. Due to intense media coverage, these recent incidents and others that have since occurred in other waters have also raised flags beyond **Europe** and **North America** and have increased awareness of these systems.[45]

For **all States**, the **2013 Snowden revelations** on government cable-tapping practices shed light on how deep governments can go in the absence of effective oversight, ushering in a slew of measures to help quell the insatiable intelligence gathering thirst of key States, and raising questions once again as to whether these measures will stand up to more recent practices.[46] In this regard, States are on alert for **cybersecurity-related incidents**, whereby State actors, or proxies working on their behalf, seek to gain access and/or create cyber–physical effects via the logical layer of subsea cable systems and electronic computer equipment and software found in the systems' dry plants and components.[47]

More recently, the February 2024 disruptions in the **Red Sea** were (yet another) wake-up call to the indirect effects of conflict and crisis on the infrastructure, particularly where maritime cable choke points are concerned. The cables were severed by the anchor of a cargo ship sunk by Houthi militants in late February, reportedly degrading 25 per cent of total Internet and telecommunications traffic between

---

41 Noor (2024).

42 According to written accounts, the first six of the 12 broken cables snapped simultaneously with the earthquake, while the next six – which lay at progressively deeper depths from north to south – then broke sequentially, from shallow to deep, over the next 13 hours and 17 minutes. Even back then, the companies that owned the cables were able to record the exact times at which each cable snapped as communication through each was lost. Importantly, research into the incident produced the first documented evidence of a turbidity current occurring in the ocean; see International Tsunami Information Center (n.d.); Derouin (2017).

43 Federal Foreign Office Germany (2024).

44 Kington (2022).

45 Blanchard and Lee (2025).

46 Broeders and Kavanagh (2023); Davenport (2015).

47 Interviews, April–October 2024; Sechrist (2012); Sherman (2021).

Europe and Asia.[48] For countries such as **Egypt** or **Djibouti** in proximity to – and highly dependent on – this maritime choke point, such incidents are particularly damaging. The incident has once again spurred much discussion about redundancy, route diversity and maintenance and repair options for the cables transiting through the area.[49]

Meanwhile, the **history of warfare and international relations**, in which cable sabotage and espionage have featured strongly, provides a legitimizing argument for many of the concerns voiced and actions being undertaken today to deter and defend against potential malicious behaviours affecting these systems. In this regard, the uptick in investments in maritime monitoring and surveillance capabilities, new doctrines such as seabed warfare first published by **France** and currently being developed by the **United Kingdom**, and the integration of critical undersea infrastructure protection into naval exercises by security organizations such as the **North Atlantic Treaty Organization** (NATO), the **Joint Expeditionary Force**, or States such as **Brazil**, **Italy** and **Portugal** provide insights into the concerns and postures of States beyond the traditional naval and signals intelligence powers.[50]

Finally, as in other areas, a growing number of governments are concerned about **economic security** and **trade risks** relevant to subsea cables. These concerns are borne out in new regulations, licensing agreements, export control and sanctions regimes, new investments in redundancy cables, or in statements on the reliability of supply chains and foreign ownership of critical system and software components, and on the availability, accessibility and reliability of maintenance and repair capabilities, not just in peacetime but also in times of crisis or conflict. **Technological** and **data sovereignty**, too, comes into play, with many States now recognizing the challenging market dynamics of new cable ownership structures in which hyperscalers or Content and Application Providers play a leading role. Many of these concerns overlap – often uncomfortably so – with competition, economic development, environmental, fishing and shipping policies, as well as with privacy and data protection, thus increasing the need for greater policy alignment and coordination within governments.

As societal dependence on subsea cable infrastructure grows in tandem with the fracturing of the international system as we know it, we can expect attention to the infrastructure to increase. Indeed, the current context suggests that subsea telecommunications cable systems need to have the capacities to withstand and rapidly recover from shocks stemming not just from traditional forms of disruption such as fishing and anchoring, or natural disasters, but also from shocks that stem from increasingly tense technological competition between the major powers; the shift to clean energy; the rush to exploit the high seas for mining and fisheries; growing instability and conflict in different maritime regions and subregions of the world; and from the extant and potential impacts of climate change. From a government perspective, considering or designating cable systems as CI can be a first step to mitigate these challenges, but as we discuss below, what really matters is what then follows in policy and practice.

---

48 Gritten (2024); Solon and Haten (2024).

49 Not the first time – the Red Sea has been a point of vulnerability for over a century, with options sought for alternative routes circulating too for over a century. Kavanagh (forthcoming 2025).

50 Autoridade Nacional de Comunicações (2023).

3.2. International policy and principle proliferation?

The number of regional or international policies and principles on subsea cable security and resilience issued over the past decade is suggestive of their growing criticality. Already a decade ago, the **Council for Security Cooperation in the Asia Pacific** published the Memorandum on the Safety and Security of Vital Undersea Communications Infrastructure. [51] The Memorandum recommended key areas for action for national governments and for regional cooperation, including the designation of national lead agencies for submarine cable issues; membership on the ICPC; the development of regional protocols to facilitate prompt cable repairs; the development of standard procedures for information-sharing and to notify other regional States of cable breaks or suspicious activity; and the conduct of tabletop exercises to deal with cable breaks and threats to cables in multilateral and bilateral exercises. Efforts are currently underway to update this memo.[52]

In 2021, drawing from decades-long experience of working with submarine cable system owners and operators, cable builders, cable maintenance providers as well as governments, the **ICPC** published a document entitled Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables.[53] Laid out in our 2023 report, it is a compendium of "recommendations developed on the basis of existing international law and policy, industry protocols and standards, State practice, and basic common sense".[54] The recommendations it puts forward are comprehensive in scope, even if they may require updating to include new examples of good practices under the existing recommendations, and due to new challenges such as cyber and supply chain security, as well as new technology offerings and government practices that can potentially enhance protection efforts.

In February 2024, the **European Commission** published a Recommendation on Secure and Resilient Submarine Cable Infrastructures, tightly linked to its White Paper on Digital Infrastructure, and complementary to EU instruments such as the European Electronic Communications Code, the Digital Operational Resilience Act, the Network and Information Security (NIS2) and Critical Entities Resilience (CER) Directives, the Cyber Resilience Act and the updated Maritime Security Strategy, as well as a number of international standards.[55] The European Commission's Recommendation proposes several actions to enhance the security and resilience of critical submarine cable systems. At the **member State level**, governments are encouraged to conduct risk assessments, map existing and planned infrastructures, and implement stringent security standards across the physical and logical layers of the systems. Regular stress testing of operators is recommended to assess resilience under various scenarios, while administrative processes for planning, construction, and repair of cables should be streamlined to ensure timely deployment and maintenance. Member States are encouraged "to consider the planning, acquisition, construction, operation, maintenance and repair of

---

51 Council for Security Cooperation in the Asia Pacific (2014).

52 Interview, October 2024.

53 International Cable Protection Committee (2021).

54 Kavanagh (2023), p.32; International Cable Protection Committee (2021).

55 European Commission (2024a; 2024c); The European Parliament (2022a–d; 2023); EU Directorate-General for Maritime Affairs and Fisheries (2014).

submarine cable infrastructures as of overriding public interest",[56] applying a broad definition to what constitutes a critical process, in line with a broad understanding of submarine cable infrastructures (discussed below).[57] At the **European Union level**, the Recommendation puts forward the need for a consolidated EU-wide risk assessment of submarine cable vulnerabilities and dependencies, supported by information-sharing and mutual assistance among member States.[58] It introduces the concept of 'Cable Projects of European Interest' aiming to address connectivity gaps, enhance resilience, and ensure geostrategic security. These projects are meant to focus on creating secure, high-capacity routes and to minimize risks related to supply chain dependencies or high-risk suppliers. To support these efforts, the Recommendation highlights the need for robust funding mechanisms that combine private investments with EU programmes such as the Connecting Europe Facility and InvestEU, with an emphasis on public–private partnerships and coordinated investments. At the **international level**, the Recommendation encourages cooperation with strategic partners and multilateral forums to promote secure and resilient global connectivity, aligning with the European Union's broader digital and economic security strategies. To facilitate implementation, these different elements have since been brought together under the **Action Plan on Cable Security**, organizing them under four pillars, notably prevention, detection, repair and response and deterrence.[59]

In October 2024 at the high-level segment of the **United Nations General Assembly**, the **United States** proposed and some 14 States endorsed a "Joint Statement on the Security and Resilience of Subsea Cables in a Globally Digitalized World".[60] Several of the principles contained therein are already covered by the ICPC Best Practices. Nonetheless, like the EU Recommendation, the New York Statement also integrates issues such as cybersecurity, supply chain security and data security that are not currently covered under the ICPC recommendations. Principles such as predictability, transparency and sustainability underpin the Statement. It is silent on another core principle – accountability.

And in November 2024, the **ITU** and the **ICPC** jointly established the International Advisory Body on the Submarine Cable Resilience, which aims to "provide strategic guidance to improve submarine cable resilience by developing best practices for protecting subsea systems and facilitating international cooperation on technical and policy frameworks". The Advisory Body is co-chaired by **Nigeria**'s Ministry of Communications, Innovation, and Digital Economy, and the National Communications Authority of **Portugal**.[61] Nigeria hosted the initiative's first summit in February 2025 resulting in a Declaration that highlights the Advisory Body's commitment to strengthen subsea cable resilience.[62]

Governments have also put in place **new security arrangements** at regional or

---

56 European Commission (2024a), p. 11.

57 Ibid., p. 9.

58 The risk assessment methodology is not set in stone, but the EC explicitly relies on the member States' feedback; ibid., p. 12.

59 European Commission (2025).

60 European Commission (2024d). The Joint Statement was proposed by the United States and originally endorsed by Australia, Canada, the European Union, the Federated States of Micronesia, Finland, France, Japan, the Marshall Islands, the Netherlands, New Zealand, Portugal, Republic of Korea, Singapore, Tonga and Tuvalu. At the time of writing, the number of countries endorsing the proposal had increased to 21, in addition to the European Union.

61 International Telecommunication Union (2024).

62 International Advisory Body on Submarine Cable Resilience (2025).

subregional levels either specifically on subsea cables or under the broader umbrella of critical undersea infrastructure, encompassing telecommunications, power cables and energy. In this regard, **NATO**'s relatively new Critical Undersea Infrastructure Coordination Cell (policy and networks) and Maritime Centre for the Security of Critical Undersea Infrastructure (operational) complement the Resilience Objectives set by the organization's members and partner States,[63] as well as other arrangements more specifically focused on hybrid or cyber warfare.

Instruments that bind all States (the **Charter of the United Nations**, **UNCLOS**, c**ustomary international law**) underpin these initiatives.[64] As a reminder of some of these obligations, in November 2023, **General Assembly resolution 78/69 on oceans and the law of the sea** reiterated the importance of protecting subsea cables as per UNCLOS, urging all States to improve their protection, given their "vital importance to the global economy and the national security of all States and their "susceptibility to intentional and accidental damage".[65] The resolution calls upon States to take measures to protect submarine cables and pipelines and to fully address issues relating to these cables and pipelines, in accordance with international law, as reflected in UNCLOS. It also encourages greater dialogue and cooperation among States and relevant regional and global organizations through workshops and seminars on the protection, laying and maintenance of submarine cables and pipelines to promote the security of such CI.[66] The resolution particularly urges States to implement their obligations regarding article 113 of UNCLOS and make breaking or injury of submarine cables or pipelines beneath the high seas done wilfully or through culpable negligence a punishable offence.[67] Further, the resolution affirms "the importance of the laying and maintenance, including the repair, of submarine cables and pipelines, undertaken in conformity with international law, as reflected in the Convention", calling upon States to "refrain from impeding the laying or maintenance of submarine cables and pipelines in a manner contrary to the provisions of the Convention, and to respect the relevant rights and duties of coastal States in the relevant maritime zones in this regard, as reflected in the Convention".[68]

Existing agreements on voluntary norms of responsible behaviour relevant to State uses of cyberspace/ICT and critical infrastructure that draw on rules and principles of international law should also be seen as applicable to State behaviour relevant to undersea cables. These include the non-binding political norms relevant to CI protection and related confidence- and capacity-building measures recommended by the **Groups of Governmental Experts (GGE)** and the **Open-ended Working Group (OEWG) on ICT/cyber and international security** and endorsed by Member States in a number of General Assembly resolutions.[69]

Finally, some of the different frameworks and proposals on subsea cable security and resilience discussed above assume that subsea cable infrastructure is (or should be) treated

---

63 The Resilience Objectives cover communications, energy, transport, health and medicine, and food and agriculture.

64 See Kavanagh (2023) relevant to the GGEs and Open-ended Working Groups on ICTs and international security.

65 General Assembly (2023), para. 175.

66 Ibid., para. 176.

67 Ibid., para. 177.

68 Ibid., para. 178.

69 The norms are 13(f), (g) and (h), as well as 13(c) and (i); see Kavanagh (2023), p.33; Kavanagh, Franken and Kulesza (forthcoming 2025).

or considered as critical, if not strategic, infrastructure.[70] The EU Recommendation and the New York Joint Statement take a more systemic approach to their interpretation of subsea cable systems. For instance, the Recommendation notes that subsea cable infrastructures include "not only cables but also any infrastructure related to their construction, operation, maintenance and repair, such as landing stations and the terrestrial parts of the submarine cable connecting to them (e.g., land routes from beach manhole to landing station, data centre, or point of presence), repair centres, as well as the fleet of deployment, maintenance and repair vessels".[71] The New York Joint Statement, issued some nine months later and endorsed by the European Union, also includes a similar description, but adds in a missing critical element: software.[72] These explanations are very useful, although the expanded understanding, which integrates a number of security risks, will likely create significant headaches for regulators, enforcement and the subsea cable industry ecosystem in years to come.[73]

3.3. From policy and principles to practice

It is evident that more and more States consider subsea cables as critical or essential to fulfilling the connectivity needs of their societies and to meeting key policy objectives and therefore subscribe to or endorse some of the frameworks discussed above. Based on our research, however, save for a few States, the difference between stated policy aims and actual practice can be as vast as the oceans through which the systems transit. For differing reasons, not all States have an understanding of how subsea cable systems work in and of themselves, or within the broader Internet and ICT ecosystem – a factor that can have important regulatory and operational consequences. Exacerbating this problem is the fact that the taxonomy used to discuss or qualify the systems and their different layers and components can vary significantly across government and industry. In addition, government policy language is often very different to that used by the owners and operators of the infrastructure and vice versa, which can lead to misunderstandings and miscommunication. This is often the case where cable damage is concerned.[74] Consider, for example, the subsea cable industry's age-old use of the terms 'external aggression' or 'external force' when a cable has been damaged, say by a ship's anchor. Pretty straightforward. Yet, for governments, the meaning of these terms can be interpreted very differently in that the terms are more generally used in reference to Charter prohibitions or thresholds relating to the use of force and self-defence.[75] For industry, government terminology can be equally perplexing.

---

70 European Commission (2024d).

71 European Commission (2024a), p. 3, para. 14.

72 Undersea cable infrastructure includes not only the communication cables themselves but also any elements related to their construction, operation, surveillance, maintenance and repair, such as landing stations, software, and the terrestrial parts of the submarine cable connecting to them, repair centres, as well as the fleet of deployment, maintenance and repair vessels.

73 European Commission (2023).

74 For example, the cable industry uses the term 'external aggression' to describe any impact that stems from outside the cable system, including anchor and fishing activity; see Ruffino (2024). However, 'external aggression' is often misinterpreted by legal or political scholars and practitioners in a narrow sense of intentional activities like sabotage or hybrid threats to cable systems.

75 For instance, Art. 2(4) of the Charter of the United Nations; General Assembly resolution 3314 on Acts of Aggression; Art. 51 of the Charter of the United Nations; or NATO's Art. 5.

Simply put, in today's geopolitical context, words shape thoughts, perceptions and actions, so should be wisely chosen by both industry and government players alike.[76] Regularly updating and disseminating relevant glossaries could be a useful contribution in this regard.[77]

Perceptions of threats and vulnerabilities also differ within a given State and between connected States, often resulting in uncoordinated responses and a mismatching of capacities, capabilities and resources. Few governments have an understanding of cable outages or damage, although this is now changing in some regions. Even fewer have access to relevant baseline data, which can lead to misunderstandings of the impact of a given incident, or how incidents are investigated, reported and attributed. The latter can also trigger misguided assumptions about how maintenance and repair capabilities should be managed and resourced. Media coverage, which has tended to be sensationalist, does not always help. Indeed, misinformed reporting can serve as fuel for malicious actors seeking to sow distrust in the systems, their owners or operators, and the States where the cables land or through whose waters the cables are passing. It also removes focus on much-needed areas of attention, such as actual hostile activity, persistent issues that lead to cable damage in specific contexts, the effects of cable damage in terms of loss of productivity and livelihoods, and where regulation, investment and innovation, as well as public–private engagement are most needed.

Regulatory and policy frameworks also tend to vary significantly across States and regions. In the best of cases, they are predictable, transparent, streamlined and expeditious. However, this is rarely the case. Highly diffuse regulatory environments create resilience issues for connected States and companies and can have far-reaching consequences in the event of multiple disruptions. Geopolitical wrangling and competition between the major powers is making regulation more complex, increasing administrative and compliance burdens for governments and businesses respectively, and at times risks undermining rather than strengthening the resilience capacities of the systems. Indeed, the recent security-driven flurry of government activity on subsea cables often appears more like a layering of new measures atop existing ones, without existing challenges such as age-old regulatory issues or common causes of cable damage being appropriately addressed. Indeed, time and time again, governments appear to have missed out on important opportunities to support more concerted and sustained efforts to resolve even the most basic of challenges.

This, too, may be slowly changing.

Significant practice regarding these and other aspects of subsea cable protection is beginning to emerge at national and regional levels, much of it thanks to some of the policy frameworks and principles discussed above, and to ever greater engagement between public and private actors. We provide some initial insights into such practice below. Documenting these practices in a more systematic manner can serve as a basis for developing national security and resilience frameworks. It can also serve as a basis for the kinds of exchanges needed between public and private actors and among States over the coming years to strengthen the security and resilience of the infrastructure, identify those practices that strengthen or undermine the latter, and move from a largely reactive footing to a more proactive and nimble one.

---

76 Franken, Schneider and Reuter (2023).

77 For instance, the ICPC has listed a glossary and abbreviations of key terms used by cable ships on its website; see International Cable Protection Committee (2024).

4. Observable State Practice

More and more governments across the world consider subsea telecommunications cables as CI and as such, are putting in place measures to strengthen the security and resilience of these systems. These measures do not (or should not) supplant in any way, the work of the subsea cable industry in ensuring the systems are built and deployed against high reliability standards that have been built up over decades and are manifest in today's state-of-the-art capabilities. Rather, government efforts should complement or enhance industry efforts to ensure the systems are both secure and resilient, by implementing protections that are already in place, through additional policy or regulatory means, investment and funding, or different forms of cooperation. As is, these efforts vary significantly across States in terms of maturity and in their treatment in policy and practical implementation. They require understanding of the systems, ownership structures, international legal and domestic regulatory issues, operation and maintenance issues, connectivity needs and nodes, data routing flows and procedures, marine spatial planning, maritime safety and security and much else, for which engagement of cable owners and operators and other critical seabed users, as well as multiple policy, regulatory and implementing bodies, is essential.

Since there is currently no organizing framework for discussing government actions as they relate to subsea cable systems from a CI perspective, we discuss them in terms of **how they contribute to key CI resilience capacities** such as the **absorptive, restorative and adaptive capacities** of the systems, and, by extension, to broader societal resilience. This framework can be fine-tuned as governments themselves refine their activity in this area. As is evident below, there is significant overlap and interaction between the three capacities.

4.1. Absorptive capacities

Absorptive capacities refer to the capacity of a system to ensure it can withstand or absorb shocks without significant loss of functionality through preventive measures and measures that can strengthen robustness and redundancy. The owners and operators of subsea cables, as well as other private entities in the subsea cable industry ecosystem, contribute to enhancing a systems' absorptive capacities in a number of ways. The systems are generally manufactured, deployed and maintained with this key capacity in mind. The majority of recommendations and standards produced by professional bodies such as the ICPC are aimed at meeting this resilience capacity. As we discuss below, governments, too, can contribute in different ways to strengthening the absorptive capacity of these systems, through a criticality designation, regulation, funding and investment, emergency preparedness, and through operational and diplomatic action. Cooperation with private actors is fundamental to each of these, even if this, too, comes with its challenges in the current geopolitical environment.[78]

[78] Noor (2024).

4.1.1. Criticality designation

A first step in contributing to the absorptive capacity of subsea cable systems is recognizing their criticality to society, the economy and national security, be that in national policy or law, or through public statements. As noted, it is often the case that private entities play an important role – at times, the lead role – in shaping how the infrastructure they own or operate is considered. The case is no different for subsea cable systems. The ICPC for years has called on governments to designate subsea cables as critical infrastructure and included a specific recommendation in its 2021 Government Best Practices.[79] In recent months, Google has called for States in Africa to consider terrestrial and subsea fibre-optic cables as CI so as to ensure better protections from a regulatory and enforcement perspective.[80] Today more and more States are taking up the issue, although there is no one way to approach it, and States will likely struggle with the all-encompassing understanding of subsea cables outlined in the EU Recommendation and the New York Statement.[81]

In terms of observable practice, based on our research, a criticality designation (or similar) for subsea telecommunications cables can be delivered through a range of instruments: a telecommunications or electronic communications act or, as is the case more recently, in legislation relating to national security, economic security, critical infrastructure, critical information infrastructure, information or cybersecurity, maritime security, computer or cyber crime, or resilience or risk and emergency management. Often, it is through a combination of these.

A designation of criticality may cover all systems landing in a given country. A designation may also be specific to a segment, site, function, service or operator, or a combination of these. For example, in some settings, submarine cable stations qualify for the highest class of asset criticality if they provide international service or connect to an autonomous region (**Portugal**) or overseas territories (**France**).[82] In other instances, a given State and its territories may only be connected internationally by one or two cables, hence any cable that lands there is, by nature, critical (**Kiribati**, **Niue**, **Cook Islands**, **Saint Helena**, **Fiji**, **Tonga**, **Shetland Islands**, **Orkney**, **Faroe Islands**).[83] This is also the case for landlocked or continental States that may not have many (or any) connections themselves but are significantly reliant on others for connectivity. In some instances, dependencies on cables going through a specific State's waters or through choke points may lead other States or regional groupings to consider those cables as critical, suggesting that certain States may need to ensure higher levels of resilience than others. In addition, a criticality designation may relate to or cover hybrid systems, that is, those systems that provide connection for offshore oil and gas facilities (**Norway**, **United Kingdom**), or for scientific research such as ocean observatories (**Norway**, **Canada**). If a key operator or its systems demonstrate sufficient absorptive capacity through redundancy options, the system (or the relevant operator) may not be considered critical or essential (**Norway**, **Spain**).[84]

---

79 International Cable Protection Committee (2021).

80 Dludla (2024).

81 European Commission (2023).

82 Autoridade Nacional de Comunicações (2019).

83 Franken, et al. (2022), p. 8–10.

84 Interview, April 2024.

4.1.2. Regulation

States commonly use regulation to protect subsea cables within their waters and to mitigate against other activities that can damage the infrastructure. In most States there is generally no single instrument for that purpose, but rather different issues are covered by different instruments. The **ICPC** Government Best Practices recommendations on regulation span the management of fishing close to cables, spatial separation, domestic cable protection laws/penalties for damage, and permitting for installation and repair. Several States are currently updating their regulatory frameworks in many of these areas (**India, Ireland, Viet Nam, United States, Comoros**). Others are, for the first time, developing them. And yet others are experiencing challenges as they develop and adapt.[85] Drawing from the ICPC recommendations, we took a closer look at some of these regulatory areas (route and landing redundancy, spatial separation, cable damage, and permitting for installation and repair/streamlining regulation), since they are particularly important for their contribution to ensuring the resilience capacities of these systems. We also delve into some of the newer regulations stemming from national security concerns.

4.1.2.1. Route and landing diversity – regulation and investment

A key way to strengthen any infrastructure's absorptive capacities is by ensuring diverse redundancy options. Redundancy remains one of the key principles underpinning the design of subsea telecommunications cable systems. This approach assumes that breaks will happen, which they do. However, most breaks go unnoticed due to the 'safety in numbers' strategy, where operators distribute their network capacity across multiple cables. This ensures that if one cable fails, the network continues to function smoothly using the others until repairs are completed.[86] For the ICPC, redundancy also involves "maximizing geographic diversity of [the] routes and landings in order to enhance network resilience and reduce the risk of damage from a single event, regardless of its cause". Governments can contribute to ensuring redundancy by "adopting and implementing regulatory frameworks to optimize routes and landings, including by ensuring geographic diversity", and by recognizing the limitations of geographical clustering of cables and of cable burial (discussed below).[87] A recent study has also highlighted the need for a more strategic approach to such cable investment planning, particularly for underserved regions. Such an approach would help identify challenges such as obstacles to financing, as well as paths forward for incentivising cable development, in financing and funding, and in collaboration around cable projects.[88]

A growing number of States are taking a closer look at redundancy issues. Some States are integrating redundancy requirements, such as cable route and landing diversity, into their regulatory frameworks, with the aim of ensuring that government and industry risk-planning baselines align on the topic. This requires a deeper understanding of dependencies, in turn a driver of some of the cable mapping initiatives underway (**European Union**).[89] In many instances, redundancy criteria are integrated into licensing or national security

---

85 Interview, WIOCC, April 2024.

86 Burdette (2024); questionnaire responses and interviews April-October.

87 International Cable Protection Committee (2021), p.6-7, para. 8, "Route and landing optimization; geographic diversity".

88 Starosielski (2025).

89 European Commission (2025), p.3.

agreements.[90] Several States fund or are seeking funding for new cable systems to enhance redundancy (**Comoros**, **Djibouti**, **France**, **Greece**, **Ireland**, **Kenya**, **Kiribati**, **Micronesia**, **Nauru**, **Netherlands**, **Portugal**, **Spain**, **Tonga**).[91] Some States have launched public consultations or tenders to identify market failure and where government intervention through funding or investment may be needed to establish new cable routes and landing sites (**Australia**, **Finland**, **Ireland**, **United States**; also the **European Union** through CEF-Digital[92] and CPEI Calls[93]). Development banks are another source of funding and investment for new or additional cables. Examples include investments by the **World Bank** in a Black Sea hybrid cable project, by the **Development Bank of Latin America and the Caribbean** in a cable between **Chile** and **Antarctica**, and by the **Asian Development Bank** in a cable linking **Palau** to **Guam**.[94] Other government drivers for strengthening redundancy include investment in back-up alternatives (microwave, satellites) and in data localization. Drawing lessons from the response to major communications outages caused by natural disasters or conflict can provide significant insights into the value of such back-up alternatives. Ensuring the capacities and resources to maintain them once deployed or installed is a challenge meriting attention, including by development banks and agencies.[95]

4.1.2.2. Spatial separation

It is recognized that **spatial separation** of submarine cables from other marine activities is an effective way to protect the cables from external shocks, thus contributing to the absorptive capacity of these systems. In addition to minimizing damage, spatial separation can ensure speedy access for maintenance and repair, critical in these times of rising tensions. According to the ICPC, States across the globe have established "default or minimum separation distances to protect submarine cables" (**China**, **Denmark**, **Russia**, **Singapore**, **United Kingdom**, **United States**).[96] These generally align with ICPC's "Recommendation on Routing and Coordinating Criteria for Submarine Telecommunications Cables in Proximity to other Such Cables', as well as relevant International Telegraph Convention provisions, and recommendations under the International Regulations for Preventing Collisions at Sea for vessels of limited

---

90 Interviews, April-October 2024.

91 Asian Development Bank (n.d.); East Micronesia Cable System (n.d.); European Health and Digital Executive Agency (2024); SEA-SPINE (n.d.); European Commission (n.d.).

92 As part of the broader Global Gateway strategy, which is intended to strengthen global connectivity aligned with EU values and standards, the EU aims to support subsea cable infrastructure 'where necessary and appropriate' through a mix of public and private financing. Leveraging existing programs such as the Connecting Europe Facility (CEF) and InvestEU, the EU provides grants and public–private partnerships to attract private investment. National Promotional Banks, the European Investment Bank, and other financial institutions should be considered in these efforts. European Commission (2021).

93 To further increase use of a cable system, the purchase of capacity for public use is another avenue that member States are encouraged to consider for supporting Cable Projects of European Interest (CPEIs). These must adhere to five criteria set out in the Recommendation on Secure and Resilient Submarine Cable Infrastructures – they are prioritized to address connectivity gaps, enhance security, and improve resilience, while contributing to the EU's geostrategic and digital sovereignty goals. European Commission (2024a). Recent CEF-Digital calls include €128 million for cables alone. European Health and Digital Executive Agency (2024).

94 Kavanagh, Franken, and Kulesza [forthcoming 2025].

95 Interviews, April–October 2024.

96 International Cable Protection Committee (2021), p. 3; interviews, April–October 2024.

manoeuvrability.[97] States such as **Ghana** are seeking to engage with other governments as well as the ICPC to understand current practice and determine the best approach for its own national context.[98]

Sometimes States opt to establish cable protection zones or corridors, prohibiting activities that could potentially cause damage to cables (e.g., fishing, anchoring, dredging). These zones or corridors tend to be either discretionary or mandatory, and enforced with air and sea patrols. The discretionary option, generally preferred by industry, "grant[s] protections to submarine cables that choose to locate in them or that may be declared around them, as in the case of **Australia**".[99] The mandatory option, as favoured by **New Zealand**, requires operators to route their infrastructure in defined geographic areas.[100] Bearing in mind its own specific realities, in 2024 the **Cook Islands** enacted the Manatua Cable Protection Act, with the aim of protecting the Manatua One Polynesian Cable, the country's only international subsea cable connection; the Act includes the establishment of two "anchor exclusion zones".[101]

The regulations establishing such protection zones generally lay out specific requirements and prohibitions, how they will be enforced (air and maritime patrols, monitoring and surveillance), as well as infringement penalties. Transparency is rendered through publication in relevant bulletins or on the relevant regulators' websites. Enforcement can often be a challenge due to a range of issues, including a lack of resources, capacities and capabilities.[102] Cable zones and corridors can also be problematic in that they may provide limited spatial separation from other cables, which can affect installation, maintenance and repair; and in that geographical clustering of cables increases the risk that "a single or man-made event could damage multiple cables".[103] In some cases, spatial issues can also be linked to physical protection of subsea cables at sea, notably cable burial, which has its pros and cons. That practice is made possible by favourable seabed conditions (soft, sandy sediment), hence the practice may not be applicable in all maritime jurisdictions. Deep burial may create challenges for repair, hence optimal burial would be at a depth sufficient to protect the cable, but not so deep as to preclude repair. For instance, due to a high volume of maritime traffic, **Singapore**, like **Hong Kong**, requires subsea cable licensees to bury their cables to a depth that can withstand an anchor drop from very large crude carriers. The required depth may be 4–12 m within port limits, depending on the condition of the sea bed and subject to approval by the Maritime and Port Authority. Beyond port limits, such as in the Traffic Separation Scheme zone, the Infocomm Media Development Authority recommends that cables be buried to be able to withstand an anchor

---

97 One nautical mile for cable ships and other vessels, and ¼ nautical mile distance from cable buoys deployed; see Sun (2018).

98 Valentia Island Symposium Proceedings Report [report forthcoming].

99 International Cable Protection Committee (2021), "Spatial Separation", para.3, pp. 3-4.

100 Ibid.

101 Parliament of the Cook Islands (2024). The two anchor exclusion zones are the Aitutake airport channel anchor exclusion zone and the Rarotonga Rutaki passage anchor exclusion zone; see relevant schedule in Parliament of the Cook Islands (2024).

102 Interview, 28 November 2024.

103 International Cable Protection Committee (2021), p.3. See also references to spatial separation and geographical clustering in the US FCC Communications Security, Reliability and Interoperability Council IV (2014), pp. 2, 5–6, 10, 14–15, 18, 30, 35, 53.

drop, especially in areas where incidents have previously occurred.[104]

Many governments are taking spatial separation more seriously than before, especially in those contexts where the potential of geopolitical risks or natural hazards are increasing, and assessing or investing in landing diversity options.[105] Sometimes, de facto cable zoning may be a side effect of policy decisions in other domains that prohibit the laying of cables in areas that are protected for environmental, cultural or national security purposes, directing subsea cable operators to route through a specific area. This underscores the need for close cooperation across policy areas and sectors.

These and other such problems have motivated some States to conduct longer-term marine spatial planning studies. One such example is an initiative of the **United Kingdom**'s Crown Estate that includes digitally mapping existing and future seabed demands out to 2050 and beyond. The proposed "integrated, spatial analysis platform" will also consider "geographical constraints for all key offshore sectors; existing infrastructure; and environmental designations as well as future resource requirements for environmental habitats and nature recovery". It will also deliver a Marine Delivery Routemap, a "collaborative initiative with partners and stakeholders to develop a long-term strategy for the marine space".[106] **Ireland** is also moving in the direction of greater policy and regulatory coordination across seabed users, aided by the establishment of the Maritime Area Regulatory Authority (MARA), a reformed Planning Commission, and a new regulatory coordination agency for the maritime space. Ireland also aims to create a centralized database for the authorization of maritime activities which could play a role in collating information and providing a better understanding of each sectors' planned activities.[107]

4.1.2.3. Charting

Damage caused to cables by commercial activity has been a constant over the past century. Charting cables for awareness can help prevent such damage.[108] The ICPC – originally established to specifically tackle cable damage – has highlighted charting-related issues over the years, noting the role that the **International Hydrographic Organization** (IHO) as well as national bodies such as the **Indian** Naval Hydrographic Office, the **South African** Navy Hydrographic Office, the Hydrographic Department of the Maritime and Port Authority of **Singapore** and the **United Kingdom**'s Hydrographic Office have played in charting cables based on data provided by cable operators. As best practices, the ICPC and other entities have recommended that governments "update nautical charts regularly and in near-real-time; show all submarine cables on nautical charts, distinguishing between in-service and out-of-service cables; show on charts all other human activities that could pose risks to submarine cables, including but not limited to mining areas, renewable energy facilities, traffic separation schemes, munitions dumps and military test areas".[109]

In terms of observable practice, governments often issue guidance or advisories – many of which stem from IHO standards and

---

104 Infocomm Media Development Authority (2019); Survey response, Singapore, October 2024.

105 Interviews, May–July, October 2024.

106 The Crown Estate (2023); Interview, September 2024.

107 Valentia Island Symposium Proceedings Report [report forthcoming].

108 Franken and Reuter (2024b).

109 International Cable Protection Committee (2021), "Charting", para. 4, pp.4-5.

resolutions – to raise awareness among other users of the sea of the location of subsea cables or pipelines on the navigational chart specifications. For instance, **The Mariner's Handbook**, published by the UK Hydrographic Office, outlines the potential hazards of damaging subsea cables, highlighting the potential consequences of their disruption not just for the delivery of critical services, but also for mariners themselves.[110] It discusses the process for charting subsea telecommunications and pipelines, and the notices or warnings that mariners receive by local and coastal radio when cables are planned, laid or when maintenance operations are underway. Once a cable is laid, the Hydrographic Office issues a notice to mariners to insert the cable on the relevant navigational charts. The Handbook also reminds mariners that it is a punishable offence in the **United Kingdom** and under international legislation to damage a cable either wilfully or through culpable negligence, although as we discuss further on, the resulting penalties are hardly a deterrent. The Handbook also reminds mariners of their obligations under the 1974 **International Convention for the Safety of Life at Sea**.[111] Complementary to this government role, industry associations such as the ICPC, the European Subsea Cables Association, the North American Submarine Cable Association and the Danish Cable Protection Committee issue recommendations promoting maritime safety and safe operation in proximity to submarine cables. Some also issue regional cable awareness charts. The Kingfisher Information Service – Offshore Renewable & Cable Awareness project (KIS-ORCA), a joint initiative between the European Subsea Cables Association and the Kingfisher Information Service of Seafish is another important example in this regard.[112]

Conversely, a number of challenges have emerged. Consider, for instance, the transition from traditional paper charts to electronic chart display and information systems (ECDIS). ECDIS represents a significant technological evolution in marine navigation, allowing automatic updates of navigational information, and reducing the manual workload and the risk of using outdated charts. However, it has created a stir in the subsea cable industry as submarine cables are not depicted at all zoom scales, thus exposing them to damage. In short, if damage occurs due to navigational decisions influenced by insufficient display or incomplete data on ECDIS, questions of liability may arise.

Due to growing concerns of cable sabotage and espionage, some in government question whether charting of all cables should be discontinued or whether cable locations should be classified.[113] For industry actors, this would place the infrastructure at an even greater risk, making it more exposed to the most common threats (fishing, anchoring, etc.). Others point to the fact that naval powers likely already chart the infrastructure for tactical, operational and strategic purposes, rendering moot the argument to discontinue the practice in nautical charts. These arguments and counter-arguments echo those that ensued in the early and mid-twentieth century. For instance, despite damage done to submarine cables by trawlers, in 1911, the British Admiralty maintained its decision not to show cables on Admiralty charts.[114] However, by the 1950s, and despite the context of the Cold War and its submarine and subsea manifestations,

110 UK Maritime & Coastguard Agency (2021).

111 International Convention for the Safety of Life at Sea, chp. V, reg. 34.

112 KIS-ORCA (n.d.); note that the United Kingdom's Seafish was formerly the Sea Fish Industry Authority.

113 Interviews, April–October, 2024.

114 UK National Archives (n.d.).

cable damage caused by commercial activity had become such an issue, including for safety at sea, that key defence agencies acquiesced to the charting of commercial cables for awareness purposes.[115] This is certainly an issue that requires careful consideration, particularly given existing international and domestic law, and the corresponding obligations and expectations for mariners and cable operators regarding cable locations.

With these and other issues in mind, the ICPC recently updated its best practice recommendations on charting, some of them specifically directed at governments and hydrographic authorities. They include: incorporation of submarine cables into national nautical charts following installation and repair; collaboration with the IHO and national hydrographic offices to ensure uniform standards in charting and data dissemination; charting of cables along their accurate alignments on hydrographic charts and chart products, with specific consideration to human activities in deeper water (e.g., deep sea mining, deep sea fishing); security considerations notwithstanding, charting seawards from at least to 10m water depth offshore; setting clear protocols for updating charts when new cables are laid or decommissioned; and supporting regional cable awareness initiatives.[116] Together with recommendations directed at cable owners and industry stakeholders as well as other maritime and offshore industries,[117] the aim is to ensure all relevant stakeholders collaborate to ensure maritime safety and protection of the infrastructure.

4.1.2.4. Cable damage penalties and enforcement

Guidance and charting are often insufficient for protecting cables from damage. From the early days, it was expected that making damage to submarine cables a punishable offence under national law would play a preventive role or serve as a deterrent. While governments might hold the same view today, the issue remains problematic, not least because of the level of inconsistency across States vis-à-vis penalties and enforcement. Articles 113 to 115 of **UNCLOS** address the protection of subsea cables on the high seas and draw heavily from the relevant provisions in the **1884 Convention** on the Protection of Submarine Telegraph Cables.[118] They are also applicable in the exclusive economic zone (EEZ) and on the continental shelf. For instance, article 113 requires States to adopt laws and regulations to provide that "breaking or injury of a submarine cable by a ship flying its flag or by a person subject to its jurisdiction beneath the high seas done wilfully or through culpable negligence" a punishable offence. In comparison to the 1884 Convention, article 113 extends the meaning of the article to apply also to conduct "calculated or likely to result in such breaking or injury". Article 114 of UNCLOS provides that States should adopt laws and regulations regarding the liability of owners of cables under their jurisdiction for the costs of repairs to existing cables which are damaged in the course of laying or repair operations. Article 115 provides that every State adopt laws and regulations to provide for an indemnity to be paid by cable owners to ship owners if they sacrifice an anchor, net or other shipping gear to avoid injuring a cable, as long as precautionary measures have been

115 Interview, May 2024; Burnett, Davenport and Beckman (2013).

116 International Cable Protection Committee (2025).

117 Ibid.

118 For a more detailed discussion on the development of international law on these topics, see Burnett, Davenport and Beckman (2013), chp. 3.

taken prior to sacrificing such gear. These provisions are interpreted and applied very differently across States.

In terms of observable actions, the ICPC highlights as best practice those measures adopted by **Australia** and **New Zealand**, for their imposition of substantial penalties for cable damage, especially in their cable protection zones. More recent examples include the **Cook Islands**,[119] which set amounts similar to those of **New Zealand**, and **France**, whereby a 2019 update to its Code imposes a fine of EUR 75,000 and a five-year prison sentence on any person who intentionally breaks – or attempts to break – a submarine cable or causes damage that could interrupt or hinder, in whole or in part, electronic communications.[120] In contrast, in 2024, **Panama**'s Maritime Authority set a much lower bar of USD 10,000 for damage caused to cables,[121] due, according to one source, to the shipping industry's 'stronghold' in the country, which risks undermining the States's digital transformation agenda goals.[122] Nonetheless, Panama's lower bar of USD 10,000 is still higher than other States that have lagged behind in updating their national legislation regarding cable damage. As widely documented, both the **United Kingdom** and the **United States** still have in place the same regulation enacted in 1885 and 1888 respectively to carry into effect the 1884 International Convention for the Protection of Submarine Cables. Fines for cable damage through culpable negligence in the **United Kingdom** still stand at an amount "not exceeding one hundred pounds" and in the **United States** to a fine "not exceeding USD 500"; fines for wilful damage, in turn, are left unclear in the UK act and set at no more than USD 5,000 in the US act.[123] As in other jurisdictions, submarine cable owners can sue for damages to their cables. A 2014 report of the US Federal Communications Commission's Communications Security, Reliability and Interoperability Council decried the limited deterrent value of the penalties for interference or damage to cables by fishermen.[124] As in **Panama**, however, the competing interests of different sea users (fishers in particular) likely come into play when addressing these shortcomings, meaning that any legislative changes to these amounts will require significant coordination and negotiation across the different sectors.[125]

Penalties for damaging subsea cables may be applied through a range of instruments. In many cases, maritime law and civil liability claims are what render a penalty. As an example, in **Canada**, according to maritime case law, "vessel owners and operators have a 'duty of care' requiring they operate their vessels prudently".[126] Under existing case law, ship owners have found it difficult to

---

119 Parliament of the Cook Islands (2024): the Manatua Cable Protection Act includes thresholds for anchor damage to submarine cables, with fines of up to NZD 250,000.

120 République Française (2019); the provisions do not apply to individuals compelled to break a submarine cable or cause damage due to the immediate necessity of protecting their lives or ensuring the safety of their vessel.

121 La Junta Directiva de la Autoridad Marítima de Panamá (2024).

122 Fígoli (2024).

123 United Kingdom (1885), para. 2 (a) and (b); United States (1888), § 1–2.

124 Communications Security, Reliability, and Interoperability Council (2014).

125 Interviews, April–October 2024; International Cable Protection Committee (2021).

126 There are reportedly at least three elements of 'duty of care': (i) an obligation to be appropriately informed of hazards to navigations through the use of up-to-date navigational charts and by consulting notices to mariners issued by Canadian authorities, which puts a corresponding obligation on cable operators to inform hydrographic authorities of the position of the cable and mariners in the area (e.g., fishers) of the presence of the cables as well as any changes to the as-laid position of the cable; (ii) an obligation not to anchor or fish in or near areas where underwater cables are located, and (iii) should they realize that their anchor or gear has snagged a cable, an obligation to drop the gear to save the cable (priority); Fontaine (2018).

avoid liability or to apportion liability to the cable owner or operator.[127] Ship owners can, however, lean on the 1976 Convention on Limitation of Liability for Maritime Claims. For instance, in the case of the Canadian-flagged vessel *The Realice*, the fishing vessel's owner tried to limit his liability for the damage he caused to a fibre-optic subsea cable (the Sunoque 1) after pulling it up and cutting it with an electric chain saw. The trial judge held the skipper liable for the full amount of damages (totalling almost CAD 1 million) for failing to consult hydrographic charts. Upon appeal, however, a Supreme Court judge confirmed that while the skipper "ran an 'unreasonable risk with subjective knowledge of that risk and indifference to the consequences', which constituted wilful misconduct", he overturned the earlier decision allowing the limitation of liability to CAD 500,000.[128]

In **Indonesia**, criminal liability for cable damage is grounded in Act No. 36/1999 on Telecommunications which "prohibits any act that may cause physical and electromagnetic disturbances to telecommunication operations and is punishable to a maximum of six years of imprisonment and/or a fine of up to IDR600.000.000" (c. USD 37,500).[129] In **China**, the criminal code is applicable. Consider, for instance, the 2023 case where a Chinese-flagged commercial vessel damaged four international subsea cables (two segments of the APCN2 cable; and two segments of the now-retired SEA-ME-WE-2 cable) in the Shantou cable protection zone. The incident reportedly resulted in estimated financial losses of more than RMB 8 million (c. USD 1.3 million). Following an investigation of the incident, the Maritime Safety Administration of **China** found that the Captain and Second Officer had demonstrated poor safety awareness and insufficient vigilance while navigating through the submarine cable zone and that their failure to detect the anchor chain's detachment led to significant damage to submarine cables and widespread communication disruptions. The Maritime Safety Administration recommended judicial proceedings against the Captain and Second Officer under suspicion of having violated Article 124 of the criminal code.[130] The Administration also recommended disciplinary actions for management failures against the shipping company's Marine Supervisor and Chief Officer, specifically for failing to fulfil their duties where safety management and anchor maintenance and repairs are concerned.[131]

In the **United Kingdom** and the **United States**, the respective Telegraph and Cable Acts include prison terms in lieu of or in addition to the aforementioned fines. The US Act does not exclude pursuit of civil liability claims by an operator in parallel.[132] In **France**, prison sentences can also be imposed along with aforementioned fines.[133] In **China**, prison sentences can range from three to seven

---

127 Ibid.

128 Ibid.; International Cable Protection Committee (2021), p. 5; see Supreme Court of Canada (2014).

129 Oktivana and Hasibuan (2024), p. 7.

130 Interview, October 2024. Under Art. 124 of Criminal Law of the People's Republic of China, any person who "sabotages any broadcasting, television or public telecommunications facility" which endangers public security risks being sentenced to a fixed-term imprisonment of not less than three years but not more than seven years. If the incident results in "serious consequences" the sentence is a fixed-term imprisonment term of not less than seven years. In the case of negligent acts, the sentence is a fixed-term imprisonment of not less than three years but not more than seven years. If the consequences of the incident are minor, the sentence is a fixed-term imprisonment of not more than three years or criminal detention. The National People's Congress (n/d).

131 Interview, October 2024.

132 United States (1888), para. 28; penalties not to bar suits for damages.

133 République Française (2004).

years, although in the event of serious consequences, a fixed term of imprisonment of not less than seven years can be applied.[134]

Two issues stand out in many cable damage cases: (i) the complexity and lengthiness of such investigations evidently increases depending on maritime location, even more so when an incident has occurred in the EEZ, continental shelf or the high seas (i.e., beyond terrotirial sovereignty); and (ii) the lengthiness of judicial proceedings. Indeed, investigating and confirming responsibility for cable damage caused by anchor dragging of a vessel underway does not just involve triaging data such from the automatic identification system,[135] vessel monitoring system,[136] sensors, radars, satellite imagery, etc., as has been the focus of many discussions relevant to cable damage incidents of late. In the event that a vessel can be boarded, it would also entail triaging that data – some of which is not always easy to access (e.g., from the vessel monitoring system), with numerous other data points such as:

- waters in which the incident has taken place;
- vessel-related information (name, size, management/ownership);
- vessel activity leading up to the incident;
- vessel inspection information (history, certification records, compliance with international maritime standards);
- ship safety inspection reports;
- vessel crew (awareness of minimal safety standards, manning for the actual voyage, crew on duty during the incident);
- certifications of top-level crew members;
- vessel maintenance and upkeep (annual/monthly maintenance schedule reports);
- ship management company information (emergency response procedures, vessel incident history, including past history of shipping accidents and application of incident prevention measures);
- actions taken by the operator;
- information on weather and sea conditions and the navigational environment;
- the incident timeline (sequencing of events before, during and after the incident);
- key incident factors (vessel identification; contact location; contact times – each of which require alignment of data points from both the cable and vessel operators);
- emergency response measures taken by the relevant operator and maritime authority (incident reporting and subsequent actions); and
- the broader context (damage of other critical undersea infrastructure in the area, cable damage trends, territorial disputes, ongoing conflict, geopolitical context, etc.).[137]

Judicial proceedings, if recommended, can take a decade or more to conclude, especially if they go to appeal. Often, cable owners reach a damage settlement with the ship owner to avoid lengthy and costly court proceedings. As witnessed in recent Baltic Sea incidents,

---

134 According to art. 124 of the Criminal Code, "Whoever sabotages any broadcasting, television or public telecommunications facility, thereby endangering public security, shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years; if there are serious consequences, he shall be sentenced to fixed-term imprisonment of not less than seven years. Whoever negligently commits the crime mentioned in the preceding paragraph shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years; if the circumstances are minor, he shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention"; Eighth National People's Congress (1997).

135 AIS is a radio-based automatic tracking system that supplements marine radar for identifying and locating vessels to prevent collisions.

136 VMS is a satellite-based tracking system used primarily for tracking and monitoring fishing vessels to ensure regulatory compliance, prevent illegal fishing, and manage fisheries.

137 List developed from interviews, July–October 2024.

a range of other complex issues such as shadow fleets and shady practices can also come into play. Despite these complexities, having in place the laws and regulations establishing cable damage as a punishable offence alongside the capacity, means and the necessary cooperative measures to conduct investigations and try such cases in a timely manner is ever more critical today.

Common standards, and possibly requirements relevant to anchor dragging by ships underway can also help. Indeed, such events can be more consequential than a ship dragging at anchor, since they can "result in the failure of multiple cables within a short period of time where cables land or are in close proximity".[138] The 2008 incident off Sicily in which an oil tanker dragged its anchor for some 300 km damaging six cables in water depths down to 180m is a case in point.[139] This and other cases suggest that recent incidents in the Baltic Sea may well have been a case of poor or negligent seamanship. Yet, the absence of agreed standards and requirements coupled with the broader geopolitical context also means that tactical manipulation of poor anchor stowage equipment or other such actions for more nefarious purposes are not in the realm of the impossible either.

In short, ensuring more effective management, oversight of and accountability for anchor-related issues of vessels underway and a meaningful response to age-old problems such as aging vessels and obscure vessel ownership[140] can help prevent many of these incidents and remove some of the room for grey zone operations that governments are rightly concerned about. This can involve steps such as standardizing approaches to securing of anchors prior to passage and at sea; ensuring port inspections following failures due to anchors, as has already been suggested to organizations such as the International Maritime Organization and to national maritime safety organizations; taking action, as suggested by the European Union, to reduce the possible impacts of aging vessels and obscure vessel ownership; and identifying the most appropriate pathways to implementing such steps.

Finally, some States, regions and organizations are also assessing means to raise the penalties for intentionally damaging subsea cables and to signal the possible consequences of such behaviour. Drawing from deterrence practice, such efforts can range from naming and shaming and countering narratives, to imposing sanctions on those individuals or entities responsible for "implementing, supporting or benefitting from destabilizing actions or policies".[141] Such actions should always be approached with the understanding that sanctions are an imperfect tool and may lead to unintended consequences.

4.1.2.5. Streamlining regulation – permitting for installation and repair

Having in place expedient permitting processes for licensing and repair can contribute significantly to strengthening a subsea cable system's resilience capacities. In most countries, contact between government entities and operators of subsea cable systems occurs through the licensing and permitting process, often through third party contractors. Based on our research, these processes can sometimes involve a wide slew of authorities and lengthy, complicated and confusing turnaround processes, which can have knock-on effects on critical operations such as laying, maintenance and repairs, undermining both

138 Green and Brooks (2011).

139 Veverka (n.d.), p. 15.

140 European Commission (2025), p. 15.

141 Ibid.

the absorptive and restorative capacities of the systems. For instance, in **Indonesia**, operators wishing to install submarine cables within the State's jurisdiction (including the EEZ and continental shelf), are subject to a permit regime involving 20 steps and several ministries and agencies.[142] In **Ireland**, the lack of a clearly defined and transparent regulatory process for landing cables in the country has been a thorn in the side of operators for years, creating challenges for planning and resourcing cable builds, a situation that becomes more challenging and potentially more costly in the current environment in which cable vessels are in high demand.[143] In the **United States**, a recent government white paper describes the challenging regulatory environment. In particular, permitting processes have made the United States "one of the most difficult countries in which to land subsea cable systems", largely due to the fact that average permitting timelines have increased from under 12 months to over three years.[144]

The ICPC has suggested that governments designate a single point of contact to streamline regulation relevant to installation and repair. Some governments already do this. For example, in **Singapore** the Infocomm Media Development Authority is the lead regulatory agency for cable landings.[145] In **Australia** it is the Australian Communications and Media Authority. In **Brazil** it is the Agência Nacional de Telecomunicações. In **China** it is the Ministry of Natural Resources (formerly the State Oceanic Administration).[146] In **Portugal**, it is the Autoridade Nacional de Comunicações.[147] In the **United States** it is the Federal Communications Commission, although informed by the so-called Teams Telecom process.[148]

Yet, sometimes, even having a single or designated point of contact or agency does not necessarily expedite the regulatory process. In both the **United States** and **China**, even with a dedicated responsible agency and process for licensing, national security concerns and tit-for-tat routing and regulatory decisions are creating significant delays in licence and permit granting at a time when demand for additional cables to meet projected capacity requirements or new national security requirements is at its highest.[149] New or strengthened rules may add to these challenges. For instance, in the **United States**, the Federal Communications Commission recently notified that it is looking to streamline procedures to expedite the submarine cable review process, a move that is much welcomed. However, the review will be part of a broader review of its Submarine Cable Landing Rules and Procedures, undertaken to assess evolving national security, law enforcement, foreign policy and trade policy risks.[150] Given the scope of the proposals to address these risks, it is difficult to see how the cable review

---

142 Oktivana and Hasibuan (2024).

143 Cf. McCabe and Flynn (2024), § 2.1, specifically the discussion of the Aqua Comms consultation submission.

144 US Department of Homeland Security. (2024), p.5.

145 Infocomm Media Development Authority Singapore (2016).

146 The *1989 Provisions Governing the Laying of Submarine Cables and Pipelines* designated the State Oceanic Administration (SOA) as the lead administrative agency for overseeing submarine cables and pipelines. In 2018, the responsibilities of the SOA were consolidated into the newly established Ministry of Natural Resources.

147 Bafoutsou, Papaphilippou, and Dekker (2023).

148 Team Telecom has been replaced by the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector. The Committee reviews submarine cable license applications as well as transactions regarding an existing submarine cable landing licenses; see **https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector**.

149 Runde, Murphy, and Bryja (2024); Wall and Morcos (2021); Petit (2024); Noor (2024).

150 US Federal Communications Commission (2024).

process can be expedited. Nonetheless, in the aforementioned white paper, the US Department of Homeland Security committed to conducting "a comprehensive assessment of cable permitting and licensing authorities" and, in support of the Federal Communications Commission's proposed regulatory updates, it will "pursue and support opportunities to enable faster, more transparent, and more consistent outcomes [in] cable licensing through enhanced but predictable security and resilience requirements".[151]

At the other extreme, **Denmark**'s approach to licensing and permitting of subsea telecommunications projects is often cited as good practice, due to its coherence, timeliness and consistency, even under a more intense security environment.[152] **France** has streamlined its own processes and in 2019 published a concise overview along with flowcharts describing what the different licensing and permitting processes entail.[153] It is expected that other EU governments will move in a similar direction, motivated by statements such as the European Commission's Recommendation on Secure and Resilient Submarine Cable Infrastructures, as well as feedback from national-level consultations and market studies. For instance, the Recommendation includes a specific item on fast-tracking permit granting procedures through the establishment not just of a single authority to facilitate and coordinate the permit-granting process, but also the appointment of a coordinator by that authority, "to serve as a single [point of contact], and convene a working group where all authorities involved in the administrative applications would be represented in order to draw up a permit granting schedule and to monitor and coordinate its implementation".[154] Some States are already moving in that direction. For instance, **Germany**, known for its lengthy bureaucratic permitting processes due to its federal system and strict environmental regulations in areas like the Wadden Sea, is striving to attract more cable infrastructure projects through improved cross-governmental and cross-level coordination, with initiatives increasingly led by the Federal Ministry for Digital and Transport.[155] Following several public consultations and internal reviews, **Ireland**, too, has started to streamline its permitting regime including through the passing of the Maritime Area Planning Act in 2022 and the establishment of the Maritime Area Regulatory Authority. The results of a 2024 consultative process led by the Department of the Environment, Climate and Communications highlights that more still needs to be done to ensure greater clarity and predictability throughout the lifecycle of the permitting process (for maintenance and repair, as well as installation) and greater alignment with UNCLOS obligations where the Irish EEZ is concerned. In the **Netherlands**, various authorities participate in a Subsea Cable Coalition, a public–private initiative established to attract cable investments, one of its sales pitches being to "streamline and optimize the permitting process for cables landing in the country".[156] In **Portugal**, the Autoridade Nacional de Comunicações has committed to introducing measures to enhance subsea cable security

151 US Department of Homeland Security. (2024), p.6.

152 Interviews April-October, 2024.

153 Secrétariat général de la mer (2020).

154 European Commission (2024a), p. 10–11.

155 Federal Ministry for Digital and Transport of Germany (n/d); Federal Ministry for Digital and Transport of Germany (2024); Eurofiber (2024).

156 The mission of the Dutch Subsea Cable Coalition is to improve the position of the Netherlands where fibre-optic subsea cables are involved. Represented in the coalition are infrastructure operators, data centres, different levels of government, knowledge institutes, and wholesale end users; see Dutch Subsea Cable Coalition (n.d.).

and repair efficiency, including a planned electronic portal to simplify licensing for installation, maintenance, and repair permits.[157]

Finally, regulators are also paying more attention to Content and Application Providers, which have evolved from major users to major owners of subsea cables. According to the European Body of European Regulators for Electronic Communications (BEREC), this may result in "increased requirements for authorization procedures in the future", likely requiring significant coordination and streamlining with existing regulation.[158]

4.1.2.6. National security, cyber security, supply chain security regulation

An ever-growing number of States are putting in place security-related standards, requirements and agreements aimed at protecting subsea cable systems, not least because of the growing number of critical national functions that rely on them. These measures, when balanced with traditional resilience measures, can contribute to strengthening the absorptive capacity of subsea cable systems. Most of these measures aim to ensure that both the physical and cyber security of subsea cable systems are hardened across all their components and that supply chains, too, are resilient in the event of disruption or interference. While the ICPC best practices do not yet cover these issues, there are many observable practices that can serve as a basis for further exchanges.

Already, there is broadening recognition of the physical and cyber vulnerabilities of cable landing stations, front and back haul,[159] points of presence,[160] and data centres. While industry action and technological developments help mitigate some of these challenges, government action, too, is often necessary. For instance, in **Singapore**, all submarine cable operators are subjected to strict security and resilience requirements, which include implementing proper access control into submarine cable facilities.[161] In **Kenya**, operators of cable landing sites and stations, which are considered critical information infrastructure under national law, are required to put in place minimum physical and technical security measures to protect the infrastructure and the data held therein.[162] In the **European Union**, under the CER Directive, critical entities, which would surely include entities in the subsea cable industry ecosystem, will have to take resilience-enhancing measures, such as ensuring adequate physical protection of their premises and infrastructure, responding to and mitigating consequences of incidents, as well as recovering from incidents.[163]

Regarding cybersecurity, the past decade has seen a significant increase in government

---

157 These measures are included in the 12 recommendations put forward by the working group on the future of submarine cables for CAM (Portugal, Azores and Madeira) communications under Order no. 4805/2019 of 13 May 2020, ANACOM (2020); see also Bafoutsou, Papaphilippou, and Dekker (2023), p. 9.

158 BEREC (2024b). For a more in-depth discussion on these issues, see BEREC (2024a).

159 In a subsea cable system, front haul and back haul refer to different segments of the network that connect users to the core Internet infrastructure. Front haul connects the cable landing station to the subsea cable system itself, while back haul extends from the cable landing station to the terrestrial network.

160 Points of presence are access points where network providers can interconnect with subsea cable infrastructure, allowing data traffic to enter or exit subsea networks.

161 Survey response, Singapore, October 2024.

162 Survey response, WIOCC, January 2025; see specifically Kenya Computer Misuse and Cybercrimes Act (no. 5 of 2018) and the supplementary Kenya Gazette notice Vol. CXXIV—No. 21 of 31 January 2022.

163 The 11 sectors identified under the CER Directive include the digital infrastructure sectors. It is the responsibility of member States to identify critical entities, carry out risk assessments and adopt resilience strategies; European Commission (2025).

action, guided by international standards such as ISO/IEC 27001, and regional and national level cybersecurity frameworks which would apply to relevant logical components, equipment and software of subsea cable systems. As previously noted, agreed voluntary norms of responsible State behaviour regarding ICTs, cybersecurity and CI would also apply to subsea cable systems.[164] Greater exchanges on adherence to and operationalization of these specific norms as they apply to the relevant components of subsea cable systems would be of value to many States.

At national level, owners and operators of subsea cable systems increasingly will be expected to comply with new cybersecurity regulations. For instance, the **European Union**'s NIS2 Directive – the core EU instrument on cybersecurity – has integrated cybersecurity as a core aspect of resilience, broadening the scope of the instrument to cover "entities that are digital infrastructure and service providers operating submarine cables".[165] Operators are expected to "protect their network and information systems as well as their physical environment from any event, including man-made damage or environmental hazards".[166] The protection of submarine communications cables is to be included in national cybersecurity strategies. EU States will need to map potential risks and mitigation measures to ensure the highest level of protection against all hazards, and identified critical entities will be expected to comply with risk-management measures and incident reporting obligations, with the latter reported to the relevant cybersecurity incident response team or competent authority.[167] NIS2 covers other obligations, where appropriate, such as providing competent national authorities with "information on planned changes in submarine cable infrastructures, and requirements for advance testing by national auditing/certification laboratories of specific IT components and systems for security and integrity purposes".[168]

On supply chains, the NIS2 Directive and the more recent EU Action Plan on Cable Security also discuss the possibility of developing a subsea cable security 'toolbox', which would set out mitigating measures for EU States to adopt in order to "reduce risks, vulnerabilities and dependencies, in particular on high-risk suppliers", identified through Union-wide risk assessments.[169] The **United States** is considering how to integrate similar supply-chain risks into its rule-making procedure, and **China** is adopting its own such measures. Meanwhile, the New York Joint Statement on the Security and Resilience of Subsea Cables includes principles relevant to suppliers and service providers that its endorsers are expected to follow.[170] Similarly, many governments are updating their foreign investment legislation to ensure that only 'trusted entities' have a stake in subsea cable infrastructure landing in or connecting to their countries.[171]

The 2024 EU Recommendation on Secure and Resilient Submarine Cable Infrastructures and the 2025 Action Plan also encourage EU States to make entities operating submarine

---

164 Kavanagh (2023), p. 33–34

165 European Commission (2025), p. 3.

166 Ibid.

167 Ibid. As a means to avoid duplication with CER Directive requirements, NIS2 requirements on risk management and reporting take precedence.

168 Ibid.

169 European Commission (2024a), p. 12.

170 European Commission (2024d).

171 Kavanagh (2023).

cable infrastructures subject to regular stress testing as a means to "assess entities' resilience under different scenarios", and proposes potential funding sources for such actions.[172] One issue that States are (or should be) stress-testing is availability of and access to spare part depots, including in the event of disaster or conflict.

Again, the challenge for many States in implementing or adhering to many of these security-related measures and principles will be ensuring that greater government control does not inadvertently undermine the resilience capacities of the very systems they set out to protect, including where route or cable landing diversity, maintenance and repair operations, and spare depots and supplies are concerned. Consider for instance the Universal Joint, which is a method of connecting all types of submarine optical telecommunication cables, regardless of manufacture, using common construction equipment and standard piece-parts in the joint as far as is practicable.[173] Organized by a small consortium of suppliers, some equipment and components of this technology are sole sourced. For some industry players, these and other such supply chain resilience issues could be further exacerbated in the event of tightened State restrictions.[174] Addressing such challenges requires strong cross-governmental coordination and effective processes for engaging with industry to understand what lies behind certain concerns and where certain measures may actually create more vulnerabilities for States.

On the regulatory front, States will need to ensure that reporting requirements that come with these additional measures are not overly complex or burdensome from a compliance perspective, or too lax vis-à-vis other resilience objectives relevant to the environment, sustainable development, privacy and data protection. And States need to consider such requirements from the perspective of their own societal and industry growth needs, ensuring that they retain agency in determining their own paths to common security and resilience goals.

Finally, the intense focus on cybersecurity and supply chains requires a more tacit acknowledgement of the age-old elephant in the room: powerful States spy on and conduct covert cyberoperations against each other, they introduce 'backdoors' into equipment via software, and they are often reluctant to restrain their freedom of action relevant to such practices. Advancements in cable technologies have rendered cable tapping in the deep seas a much more complex endeavour, shifting attention to network management systems and software, equipment and terrestrial access points (cable landing stations, points of presence, data centres) where malicious actors have easier access to the data flowing through the systems as well as ample room for pre-positioning. A more frank discussion on such issues, including the equities involved and what they mean for the resilience capacities of systems deemed vital to our economies and the general well-being of society, is perhaps overdue. So, too, is a conversation on disruptive technologies (such as quantum communications and quantum key distribution) and what they will mean for future subsea cable security and resilience efforts.[175]

---

172 European Commission (2024a), pp. 2–3. Such testing actions could be supported financially by the Digital Europe Programme, in particular under the DEP cybersecurity work programme 2023–2024; see European Commission (2021).

173 See https://ujconsortium.com/information/what-is-universal-jointing.

174 Valentia Transatlantic Cable Foundation (2024); written communication with industry representative, January 2025.

175 See, for instance, euNetworks (2023). While still in its early development, quantum key distribution is believed to significantly enhance communication security by leveraging the principles of quantum mechanics to generate and exchange encryption keys securely between parties.

4.1.3. National policy coordination arrangements

Having in place a **national structure** or mechanism for **coordinating government policy and action** on subsea telecommunications cables and for pulling together the different initiatives that aim to ensure the systems can withstand, absorb or respond to shocks is a key element of resilience. Conversely, putting in place such **coordination arrangements** can be complex. In our 2023 report we discussed how subsea cable systems do not fit neatly into one policy area, but rather straddle a number of regulatory, policy and operational authorities and entities.[176] Similarly, threats and vulnerabilities can manifest across the different layers and components of the architecture, which itself is rapidly changing. The ICPC has noted how a wide dispersion of responsibilities for subsea cables can work against government action with regard to subsea cables, including where interaction with other policy areas and other actors might be required. As evidenced in the interviews conducted for this study, some governments are confronting this challenge by **designating a lead department or entity** to coordinate government action on subsea cable security and resilience issues at policy level, while respecting the core responsibilities and functions of other key entities or authorities. The policy lead may be responsible for coordinating with other government entities on overlapping policy questions (e.g., energy, the environment, fishing, shipping, cybersecurity, deep-sea mining, national security, diplomatic initiatives). In some instances, it may also be the lead or the main point of contact for reporting of incidents of national or cross-border significance.

The **United States**, like many of the States mentioned in this report, realizes that it would benefit from "improved internal coordination" for a more strategic approach to subsea cable security and resilience.[177] In **Singapore**, the Infocomm Media Development Authority is the lead government entity on subsea telecommunications cables, serving as a 'one stop shop' to interface between government agencies and operators.[178] In this role, and as a means to meet one of the strategic priorities laid down in its 2023 Digital Connectivity Blueprint, which is to "provide capacity to enable submarine cable landings to double within the next ten years", the Authority works closely with local government agencies and industry to identify suitable new sites and cable corridors for cable landings and to facilitate the landing of new cables.[179] It serves as the lead agency for domestic policies and regulations to enhance cable protection and resilience and on international engagement and cooperation relevant to submarine cables. In the **United Kingdom**, while regulatory issues are still dealt with by the Crown Estate and the Marine Management Organisation, the Department of Science, Innovation and Technology has been designated as lead for telecommunications, data and Internet infrastructure policy, including the subsea telecommunications cables connecting the country to the global Internet. As such, the Department has established dedicated functions with specific coordinating and reporting responsibilities across government authorities and policy

176 Kavanagh (2023), p.17.

177 Department of Homeland Security (2024), p.6.

178 Survey response, Singapore, October 2024.

179 Infocomm Media Development Authority (2023), p.13.

areas.[180] Like many entities in other States, the Department is seeking to develop an evidence base to inform policy development on subsea cable-related issues.[181] In **France**, as in many States, the designation of a national coordinator for submarine communication cables is tied to the State's efforts to attract more cable landings. The role has been assigned to the Interministerial Mission for the Acceleration of Industrial Developments, which is attached to the General Directorate for Enterprises within the Ministry of Economy and Finance. Its main responsibilities involve facilitating relations with industry, including with regard to administrative procedures; and supporting territorial services, notably to ensure that projects are implemented in compliance with applicable regulations and inter-service coordination. The latter applies to overseas territories and to cable projects which involve foreign governments or companies.[182]

Often, a policy lead or national coordinator may also be the lead entity for international engagement on subsea telecommunications cable issues, as in the case of **Singapore**. In other contexts, that outward-facing role is increasingly taken on by ministries or departments of foreign affairs, as is the case of **Australia**'s new **Cable Connectivity and Resilience Centre** and the **US Department of State**'s Bureau of Cyberspace and Digital Policy.[183]

4.1.4. National preparedness

Related to the above, for a growing number of States, a consideration of 'criticality' also provides a basis for integrating subsea infrastructure into national (or regional) preparedness and crisis response arrangements. Already in 2014, a **Council for Security Cooperation in the Asia Pacific** memorandum proposed that governments in the region establish a number of cooperative mechanisms in order to protect submarine cables and ensure their rapid repair.[184] One such measure included 'contingency planning at the regional level' which would include "a standard procedure whereby the cable industry immediately notifies relevant government agencies through *a designated national lead agency* wherever there is a cable break or suspicious activity observed so that a risk assessment can be conducted to determine the likelihood of a possible hostile action".[185] In this regard, the memorandum emphasized the need to prioritize the designation of a lead agency for cables, which, as discussed above, some States in the region such as **Singapore** have taken seriously.

Today, many States now consider subsea cable incidents in their national emergency preparedness plans, are establishing crisis coordination arrangements within and between relevant States, as well as dedicated points of contact at policy and operational

---

180 Some key government entities that DIST engages with specifically on subsea cable issues and incidents include the Cabinet Office, the National Protective Security Authority on physical security issues; the National Cyber Security Centre on threats to the logical layer of cable systems; the Ministry of Defence, which is operational lead for monitoring activity within UK territorial waters and its EEZ; the Maritime and Coastguard Agency; and the Joint Maritime Security Centre and its National Maritime Information Centre, which are responsible for providing Maritime Domain Awareness and Understanding to all of government and UK law enforcement, in turn underpinned by the Royal Navy's Maritime Domain Awareness Programme which provides the essential data layer to the Joint Maritime Security Centre. Some of these existing structures are also reviewing their policies and updating their reporting systems relevant to subsea infrastructure.

181 UK Department for Science, Innovation & Technology (2024).

182 Secrétariat général de la mer (2020), para. 2.2.

183 Australia Department of Foreign Affairs and Trade (n/d); US Department of State (2024b).

184 Council for Security Cooperation in the Asia Pacific (2014), p. 3.

185 Ibid. (emphasis added).

levels. They are also beginning to put in place the necessary mechanisms and procedures to ensure coordination of response and operational preparedness to incidents affecting the infrastructure. For instance, in the **United Kingdom**, the Department of Science, Innovation and Technology has established a 'subsea communications cable industry group' which meets regularly on a voluntary basis to discuss different issues, including potential risks to the systems. The group includes tier 1 companies, and other traditional industry actors. Depending on the topic discussed, a given meeting may involve other key government or industry actors. Key issues that the group has focused on recently include crisis communications. In this regard, exercises with government and industry actors have been used to confirm and test roles and responsibilities of different actors from incident reporting through to response and recovery. In addition, the Department engages in a range of cooperative mechanisms with counterparts in other States, many of which relate to exchanging information on policies and sharing information on incidents.[186]

Often these kinds of efforts begin with consultations or outreach to industry. For instance, in December 2024, **Ireland** and **Iceland** convened government and industry representatives and researchers to deepen their understanding of different aspects of crisis management as it applies to subsea communications cables and to inform their own national processes and procedures relevant to contingency planning, incident reporting, crisis response and crisis communications. Within its current regulatory review, the **United States**' Federal Communications Commission has sought comment on how the Commission can facilitate information-sharing between national security agencies and industry.[187] For its part, following an initial series of engagements between government departments and leading subsea cable owners, operators, vendors and suppliers, the Department of Homeland Security has committed to enhance mechanisms for more effective coordination with the subsea cable industry ecosystem.[188]

In the **European Union**, member States can use a number of instruments as guidance for preparedness and crisis management relevant to subsea infrastructure. The most recent of these is the Critical Infrastructure Blueprint, which provides a basis for a coordinated Union-wide response to disruptions of CI with significant cross-border relevance,[189] and the proposed EU Blueprint on cybersecurity crisis management, which will cover crises resulting from large-scale cybersecurity incidents affecting network and information system availability for sectors covered under NIS2.[190] These need to be tailored and coordinated with other key EU instruments such as the Council's Integrated Political Crisis Response Mechanism,[191] the Working Party on Civil Protection (PROCIV) which covers critical infrastructure, the updated Maritime

---

186 Interviews April-October 2024; Valentia Island Symposium Proceedings Report (forthcoming).

187 This was consistent with consistent with an April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience, which noted with regard to information-sharing: "The appropriate sharing of information, which may include relevant classified and unclassified intelligence and [law enforcement] sensitive information, among Federal, State, local, Tribal, and territorial entities; owners and operators; and other relevant stakeholders, is essential for effective risk management. The Federal government will support a robust information sharing environment and public–private cooperation that enables actions and outcomes that reduce risk"; US Department of State (2024a).

188 US Department of Homeland Security (2024); see section on Public–Private Engagement, Path Forward, p. 6.

189 European Council (2024).

190 European Commission (2025b).

191 European Council (2020).

Security Strategy,[192] as well as the broad range of other crisis management instruments and networks already in place.[193] The recent EU Action Plan on Cable Security also calls on EU States to "make effective use of existing incident reporting mechanisms under the CER and NIS2 Directives and avail of contact lists provided for in the aforementioned Blueprints".[194]

While progress on transposing many of these instruments into national legislation is fitful, it should eventually allow for a more coordinated response to potential incidents. **Ireland**, for example, introduced new regulations in October 2024 to transpose the CER Directive into national law. The new regulations include a provision for a Minister with responsibility for a particular sector to potentially provide financial assistance to a Critical Entity or a Competent Authority where an essential service needs to be supported and such support is justified by public interest objectives.[195] It is not yet clear whether the provision would apply to subsea telecommunications cable systems in an Irish context and whether the provision mentioned would ever be triggered in the event of an incident. Nonetheless, this provision and others complement key cyber crisis management and incident response provisions relevant to digital infrastructure (under which subsea cables and data centres fall) in the forthcoming National Cyber Security Bill, which will transpose the NIS2 Directive into national law.[196] Ireland's first national maritime security strategy, currently under development, will likely also cover such issues. For EU States that are also members of NATO or that participate in loose coalitions such as the Joint Expeditionary Force, other mechanisms likely also kick in, particularly in the event of incidents in which the involvement of hostile State actors is suspected. One recent example is the Joint Expeditionary Force's UK-led reaction system Nordic Warden which will track threats to undersea infrastructure, monitor shadow fleets and alert partner States and NATO in the event of suspicious activity. Another is NATO's Baltic Sentry, which aims to "enhance NATO's military presence in the Baltic Sea and improve Allies' ability to respond to destabilizing acts".[197]

4.1.4.1. Understanding and managing risk

Understanding risk is key to emergency preparedness and crisis management and should be a key driver for a government's contribution to strengthening a system's resilience capacities. Most damage to subsea cables stems from commercial activity and natural hazards, largely occurring in a country's territorial sea, often in shallow or congested waters. These kinds of risks, which also manifest differently depending on geography, are what tend to keep industry players up at night and many of the government best practices identified by the **ICPC** have been penned with these in mind. Increasingly for many governments, however, it is also the intentions of malicious State actors (or proxies acting on their behalf) vis-à-vis subsea cable systems that concern them. As a result, governments have been calling for greater understanding of the risks associated

192 European Council (2023).

193 These include the EU Hybrid Toolbox and the revised EU Protocol for countering hybrid threats, the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), the CSIRTs network and the pan-European systemic cyber incident coordination framework for relevant authorities (EU-SCICF).

194 European Commission (2025), p. 13.

195 Statutory Instruments, S.I. No. 559 of 2024, European Union (Resilience of Critical Entities) Regulations, para. 6.

196 A Cabinet decision in July 2024 directed priority drafting of the legislation transposing the NIS2 Directive, and drafting is underway; Department of Environment, Climate and Communications (2024).

197 UK Ministry of Defence et al. (2025); NATO (2025).

with subsea infrastructure to enhance incident or crisis preparedness. As noted, the **European Commission**'s recent Recommendation has emphasized the importance of risk assessments and mapping,[198] as has the New York Joint Statement on the Security and Resilience of Undersea Cables.[199] In the **United States**, the FCC's proposed regulatory changes are strongly centred on risks not previously contemplated, among them national security, foreign policy and trade risks.[200] The US Department of Homeland Security white paper, too, emphasizes risk, being particularly concerned with those that may occur in the deep sea.[201]

The ICPC Best Practices suggest that governments "focus on statistically-significant risks where government action could have the greatest impact on risk reduction" and that governments "consult closely with industry to understand industry technology and operating parameters and to share data regarding risks".[202] The recommendations note the utility of such a practice for "identifying patterns of activity, gaps in existing cable protection efforts, areas for improving resilience, and identification of malicious acts by States and non-State actors".[203] As a best practice, the ICPC therefore suggests that "consistent with competition laws, [governments consider] establish[ing] mechanisms for exchanging incident data and threat information".[204] Under its CI designation recommendation, the ICPC also suggests that governments "gather and assess data regarding vulnerabilities of, and threats to, submarine cables" and "develop and implement policies to reduce those vulnerabilities and threats".[205] Transposing these recommendations on data-sharing and risk assessment into actual practice is no easy task and can become entangled in a web of commercial and national political and security interests. Nonetheless, as noted, several governments are currently reviewing and streamlining their industry engagement processes to determine *who* on the private sector side they should engage and *for what purpose*, the *kind of data* that would be useful to governments in such exchanges, and vice versa, and *how* information can be shared in a secure manner.

In **Sweden**, until recently, such interaction with relevant industry actors was voluntary, implemented through the National Telecommunications Coordination Group. Following a broader internal review process linked to the transposition of key EU instruments (NIS2, CER) into national legislation, and the October 2023 incident in the Baltic Sea in which a subsea telecommunications cable connecting to Estonia was damaged, such interaction has now become mandatory.[206] Through their CI legislation, **the Netherlands** and **Finland**,

---

198 The Recommendation strongly emphasizes the need to develop a consolidated Union-wide assessment of risks to the infrastructure, and to this end, encourages national governments "to carry out an assessment of risks, vulnerabilities and dependencies affecting subsea cable infrastructures, which should include a mapping of existing and planned infrastructures". A tender has since been put out seeking consultants to fulfil these tasks; see European Commission (2024b).

199 The Joint Statement emphasizes the importance of regular security risk assessments across the cable life cycle, as well as the importance of considering both technical and non-technical risk factors in the development and implementation of risk mitigation measures. European Commission (2024d),

200 US Federal Communications Commission (2024).

201 Department of Homeland Security (2024), p.3.

202 International Cable Protection Committee (2021), p. 1.

203 Ibid., p. 11.

204 Ibid.

205 Ibid., p. 10.

206 Interview, 26 April 2024.

too, are providing a legal basis for such cooperative interaction with industry actors, which can help in establishing common baselines on risk.[207]

The **United States**, too, has recognized that close coordination with subsea cable industry players is key to meeting resilience challenges and objectives. Yet, as noted in the aforementioned Department of Homeland Security white paper, subsea cable systems do not fit within "existing government mechanisms for engaging critical infrastructure owners and operators". While some industry players might be represented in some existing mechanisms, there is "no forum in which the full scope of the cable industry can effectively collaborate with the U.S. government to identify and address shared challenges", in turn "limit[ing] the government's opportunities to gain insights from the cable industry on its unique risks and challenges".[208] The Department of Homeland Security committed to addressing these engagement and representation issues, including by availing of existing mechanisms and by exploring new ways to engage industry, including for "classified and unclassified information exchange".[209] Significant coordination across current review processes will be key to moving forward on this topic at all levels of government and administration.

4.1.4.2. Outage and incident reporting

As with other critical areas, governments can use incident or outage reporting to enhance understanding of risk and to enhance resilience. Having in place such mechanisms, be they mandatory or voluntary, can contribute to strengthening both the absorptive and restorative capacities of the systems. They are generally put in place to help address shortcomings vis-à-vis preventable incidents and to prepare for unexpected events. They can include defining the scope for covered entities; establishing outage thresholds; defining reporting timelines, and, in the case of mandatory reporting, ensuring enforcement in the event of non-compliance.

Incident reporting can also help to inform the establishment of baseline criteria for incident classification based on the scale and severity of an incident, a routine aspect of risk management. Incident classification, in turn, helps to generate an evidence base for understanding the threat landscape and for maintaining shared situational awareness within governments and between governments and private sector actors. Reporting also helps to identify trends where tactics, techniques and procedures are concerned, a key aspect of attribution. Reporting supports emergency preparedness and crisis management by providing a routine and consistent mechanism for objectively assessing and prioritizing incidents, identifying gaps in existing protection efforts and defences, and ensuring a timely response and recovery.[210] Moreover, such mechanisms can inform decision-making at the highest levels, and help to clarify the entity(ies) responsible for leading or coordinating the response, as well as identify relevant resources, capacity and capability requirements. Importantly in the current environment, reporting can help to ensure consistency and clarity in the way an incident is communicated within and across organizations, to the broader public or to suspected perpetrators.[211]

In some countries, subsea cable incident reporting is **informal** or **voluntary**, like for

---

207 US Department of Homeland Security. (2024).

208 Ibid, p.6.

209 Ibid.

210 Kavanagh (2022).

211 Ibid.

instance, in the **United Kingdom**. Subsea cable incidents that have national implications may get reported to the Department of Science, Innovation and Technology's telecoms incident response team, which has a dedicated officer who works on response coordination across government, although that lead role would likely delegate to defence if suspected to be the action of a hostile State actor. Today, a growing number of States are moving in the direction of **mandatory incident/outage reporting**, in accordance with specific criteria and thresholds (**Australia**, **Cook Islands**, **Estonia**, **New Zealand**, **United States**). Several States that mandate cable incident reporting also impose penalties when an incident has not been duly reported (**Australia**, **Cook Islands**, **New Zealand**, **United States**, **Uruguay**). Sometimes the notification process is tied to permitting processes for repair when disruption has occurred within a State's territorial waters or EEZ. For instance, **Singapore**'s Infocomm Media Development Authority requires notification by licensees of 'cable damage incidents' that have occurred in its Port Limits and its Traffic Separation Scheme zone. The Authority provides a standard schema for incident notification in a dedicated guidance note.[212] Given delays that permitting for repair can entail, the Maritime Port Authority of Singapore has committed to processing approvals for expedited repair works within 3–5 working days.[213] As we note further on, industry bodies have for long promoted pre-authorization for repairs, so as to avoid such delays, and some States today provide for such pre-authorization or full exemptions.

Worthy of note is the **United States** current reporting requirement set out in the **Code of Federal Regulations** – the **Network Outage Reporting System**). The reporting system focuses on submarine cable outages, whereby 'outage' is defined as a "failure or significant degradation in the performance of a licensee's cable service regardless of whether the traffic can be re-routed to an alternate path, where (i) an outage of a portion of submarine cable system between submarine line terminal equipment (SLTE) at one end of the system and SLTE at another end of the system occurs for 30 minutes or more; or (ii) an outage of any fibre pair, including due to terminal equipment, on a cable segment occurs for four hours or more, regardless of the number of fiber pairs that compromise the total capacity of the cable segment".[214] In the event of outages requiring reporting, the licensee (or a licensee representing a consortium) is expected to provide the Federal Communications Commission with a Notification, an Interim Report and a **Final Outage Report**, each within specified timelines and using specified templates.[215] The Code also provides detailed guidance on the information that should be included in each of these reports. For instance, the **Notification Report** is due within eight hours of the time of determining that an event is reportable and should include the name of the reporting entity; the name of the cable and a list of all licensees for that cable; the date and time of onset of the outage, if known; a

---

212 The schema requires the contact details of the relevant government point of contact to whom the notification should be sent, and the sections for different information that the licensee should provide (the name of the licensee; date and time of the report; the affected system; estimated date/time of damage; map coordinates (latitude and longitude); description of the incident; and any other remarks (e.g., information of the vessels in the area at the time of the incident); Infocomm Media Development Authority Singapore (2019).

213 Ibid.

214 The Code (Title 47) is also specific about what does not need to be reported, for example, if the outage is caused by announced planned maintenance and the licensee notified its customers in advance of the planned maintenance and expected duration, although there are also exceptions to this rule. US Office of the Federal Register (2024), § 4.15, para. (a).

215 Ibid. para. (b).

brief description of the event, including root cause if known; nearest cable landing station; best estimate of approximate location of the event, if known (expressed in either nautical miles and the direction from the nearest cable landing station or in latitude and longitude coordinates); best estimate of the duration of the event, if known; whether the event is related to planned maintenance; and a contact name, contact email address, and contact telephone number by which the Commission's technical staff may contact the reporting entity.[216] The **Interim Report**, due within 24 hours of receiving the Plan of Work, requires the same information as the Notification Report, as well as the "best estimate of when the cable is scheduled to be repaired, including approximate arrival time and date of the repair ship, if applicable".[217] The **Final Outage Report**, due seven days after the repair is completed, should, in addition to the data points provided in the first two reports, include information on the **outage restoration method** and be updated if further information on the outage comes to light after the report is submitted.[218]

For its part, in the **European Union**, NIS2 and CER Directives, the Critical Infrastructure and Cybersecurity Blueprints, the Digital Operational Resilience Act and other instruments provide guidance to EU States for reporting on incidents. The Recommendation and the Action Plan on Cable Security also encourage member States to share information on incidents and incident response, and on relevant best practices, in a manner that seeks to maximize synergies with the NIS2 and CER Directives.[219] The Recommendation also encourages EU States to offer each other assistance in the event of an incident,[220] while the Action Plan calls on private entities to enhance reporting of incidents, including by sharing information on incidents above and below the legal reporting obligation.[221] At a practical level, the States and operators affected by the 2023 and 2024 incidents in the **Baltic Sea** have demonstrated the usefulness of sharing incident data and of coordination and mutual assistance, even if the operators were responsible for the actual response and recovery effort and despite initial contrasting communications on the incident by those involved.[222]

4.1.4.3. Incident response

Even with clear reporting procedures and protocols in place, responding to an incident can be a messy process for governments, especially at the outset. Take the **2022 Shetland Islands incident**, in which two Faroese Telecom cables were severed. In this specific case, the Police declared a major incident after SHEFA-2, the main subsea cable between the Shetland islands and the UK mainland, was cut, affecting more than 20,000 people on the islands, including emergency services.[223] The cable operator reported the incident to the **United Kingdom**'s Maritime and Coastguard Authority, the government agency responsible at operational level for reporting in instances

---

216 Ibid, para. (b), (2), (ii).

217 Ibid. para. (b), (2), (iii).

218 Ibid. para. (b), (2), (iv).

219 European Commission (2024a), p. 12.

220 Ibid.

221 European Commission (2025), p. 11.

222 Interviews, February, April 2024.

223 McBride (2022).

where subsea cables are damaged.[224] In this case, the Authority quickly confirmed that the break resulted from anchor dragging by a UK-registered fishing vessel. The vessel in question had not reported the incident, as per its obligations.[225] However, the Coast Guard identified it as the only vessel in the area of the cable when it was damaged and could thus attribute the incident to the vessel in question – later confirmed by VMS data. While incident reporting procedures appear to have worked at the operational level, a redacted email exchange obtained by BBC Scotland through a Freedom of Information request on the incident demonstrates the complexity of incident reporting at the policy level, with a growing number of regional and national actors seeking to confirm that the cable damage had been caused by a fishing vessel and not by a hostile State actor.[226] As we discuss further on, learning from these kinds of incidents is key to national preparedness and emergency management planning.

Moreover, across almost all the States interviewed or studied, given increasing data sources and reporting requirements, efforts are underway to understand how these come together or are fused to inform not just situational awareness but also to guide decisions around the actual response. This is one particular area where additional effort to bring security and resilience together within a common framework would be very beneficial. For instance, in some recent incidents where sabotage was suspected, there has been a significant gap between the effects of the cable breaks per se, which appear to have had minimum service impacts and thus limited effects on the affected societies' vital functions, and the responses to them. Due to the geopolitical context and the strategic locations of where the incidents occurred, as well as their continued occurrence in subsequent months, the traditional law enforcement operational response (generally involving coast guards) has sometimes been accompanied by special forces, warships and other capabilities as well as significant diplomatic engagement and much else. This is not to say the latter was not warranted. Rather, as has been discussed, ensuring mechanisms for learning from these incidents should be part of national processes for reviewing and fine-tuning emergency management and response planning, military operations and related rules of engagement, and, importantly, criminal investigations and attribution processes.

---

224 Telecommunications is a reserved matter in the United Kingdom (and several other States) meaning that the central government is responsible for regulation, policy and all other telecommunication-related initiatives, including incident reporting.

225 The Scottish Government received confirmation from the Maritime Coastguard Agency on 20 October 2022 that a UK registered fishing vessel was the cause of damage to the subsea cable affecting telecommunications on Shetland; Wishart (2022).

226 In the Shetlands case, the Critical Infrastructure Resilience Unit in the Scottish Government's Resilience Division was the regional lead coordinating information and liaising with the relevant Scottish and central governments on the incident.

4.2. Restorative Capacities

Restorative capacities refer to the capacity of a system to re-establish performance as quickly as possible after a disruptive event. It involves actions that are carried out to revert the effects of a disruption. It is enhanced by contingency plans, competent emergency operations, and the means to get the right people and resources to the right places. These are measures generally taken by the owners and operators of the systems and other private actors in the ecosystem. Yet, governments, too, can often contribute to strengthening the restorative capacities of the systems. Our research shows that these efforts can manifest through regulatory action, investments in knowledge development and metrics, in maintenance and repair capabilities, and in crisis response.

4.2.1. Regulation

For the ICPC, a key step that governments can take to ensure that the performance of a cable system is restored as quickly as possible is ensuring that national regulation does not cause unnecessary delays to repair efforts, be it because of permitting or port entry requirements, the imposition of cabotage and crewing restrictions, maritime boundary claims and disputes, or the imposition of importation requirements and custom duties.[227] Nonetheless, government practice across each of these areas varies enormously, further complicated at times when one government authority makes a decision that contradicts that of another. There may also be regulatory inconsistencies across the jurisdictions through which a cable crosses or on which it lands, which can create significant delays to maintenance and repair efforts. For instance, **Canada**, **China**, **Indonesia** and **Malaysia** are often called out by industry for their cabotage practices. As a case in point, administrative red tape and the cabotage regulations in **Indonesia** meant that repairs of the SEA-ME-WE 5 cable damage in 2024 took several weeks, rather than just a few days, to repair.[228] **Malaysia** recently changed its cabotage policy for foreign ships for installation and repair. The decision resulted from "significant pressure from local and international tech players, as well as the government's own commitment to advance the country's digital transformation agenda".[229] In **China**, in accordance with art. 70(6) of the Marine Environment Protection Law, foreign vessels are required to obtain prior approval to enter China's territorial sea to repair, adjust, or remove its subsea cables. Conversely, a later regulation allows foreign maintenance ships to act where urgent repairs are required for damaged cables laid on China's continental shelf, provided that such operations do not "impair China's sovereign rights and jurisdiction".[230]

As noted earlier, streamlining regulation and identifying a designated point of contact for regulatory and policy issues can help to overcome these challenges. In some regions, industry and governments are collaborating to raise awareness of these challenges and to promote greater consistency and coherence in relevant regulation. Oftentimes, governments have legitimate reasons to impose restrictions, yet provide workarounds to allow expedited access for maintenance and repair.

---

227 International Cable Protection Committee (2021).

228 Noor (2024).

229 Noor (2024), p.6.

230 State Council of the People's Republic of China (1989).

Singapore, which has not experienced any cable cuts in its own waters over the past three years, is concerned about reports that "cable repairs around the world, in particular faults at sea, have taken longer than usual to repair/resolve, thus hurting consumers and businesses that depend on the cables for their connectivity needs".[231] Understanding that repair times to resolve cable faults depend on a number of factors, for Singapore "it is critical that the global community, including governments and private sector, work towards consensus on norms and standards to protect this critical undersea infrastructure, and ensure timely restoration on international connectivity lifelines".[232] We come back to some of these issues below.

4.2.2. Identifying investment and other such gaps

A robust maintenance and repair ecosystem is key to ensuring the restorative capacities of the global network of subsea cable systems. Until relatively recently, few States had a clear understanding of this niche area of the industry and how it keeps data flowing between continents, even in the event of serious disruptions, or during global crises such as COVID-19. Today, triggered by growing dependencies on the systems and concerns of their vulnerability to serious outages, numerous States are turning their attention to the resiliency of the maintenance and repair ecosystem and the measures they, too, may need to take to enable and ensure sufficient maintenance and repair capabilities, secure the supply of spare cables, material and equipment, and sustain the niche cable maintenance workforce.

Most policy and regulatory attention has focused on ensuring accessibility to core cable suppliers and to cable repair capabilities, including in times of crisis and conflict, and to ensure that these services, too, are both secure and resilient. To this end, some States are conducting in-depth consultations and studies to support policy and regulatory development in this area and assess whether they may need to fill investment gaps. For instance, in 2023, the **United Kingdom**'s Department of Science, Innovation and Technology issued a public tender to assess the maintenance and repair structures and provisions for the United Kingdom, which is highly dependent on subsea cables, although boasting high levels of resilience.[233] Through the tender, the Department sought to understand opportunities and challenges of the extant model, what "a sustainable and effective repair model" looks like in practice, as well as potential vulnerabilities in the event of a major outage leading to unacceptable disruption.[234] **India**, too, has increased its focus on the topic, with a 2023 in-depth study undertaken by the Telecom Regulatory Authority highlighting the lack of a sovereign repair capability as a major vulnerability in light of its connectivity needs and its digital transformation objectives.[235]

States of **West Africa**, affected first by the Red Sea outages in February 2024 and shortly thereafter by those resulting from the undersea event off the coast of Abidjan in Cote d'Ivoire, were concerned enough to raise the topic at the ITU, and push for the establishment of an international advisory group to study "the timely deployment and repair of submarine cables".[236]

---

231 Singapore questionnaire response, October 2024.

232 Ibid.

233 Franken et al. (2022).

234 UK Department of Science, Innovation and Technology (2023).

235 Ministry of Communications, India (2023).

236 International Telecommunication Union (2024).

Some States have already made investments. Indeed, as already discussed in our 2023 report, in 2019, the **United States' National Defense Authorization Act** for Fiscal Year 2020 provided for the establishment of a "**Cable Security Fleet**".[237] The Fleet includes two commercial vessels already providing (or being built to provide) cable services such as "installation, maintenance, or repair of submarine cables and related equipment, and related cable vessel operations".[238] The relevant Code provides strict criteria regarding the age and flag of the vessels, the citizenship of the owner and operator of the vessel, and chartering of the vessel. It also sets out obligations and rights under operating agreements, as well as a long list of national security requirements and a payment schedule of USD 10 million per annum.[239] The **United States**' backing of SubCom as a core supplier to countries in the strategic East Asia Pacific region, and **France**'s recent (re)purchase of majority shares in Alcatel Submarine Networks, one of the other main cable suppliers, and its framing of the acquisition as a strategic move, signals the value of these companies today.[240]

In its Recommendation on Secure and Resilient Submarine Cable Infrastructures, the **European Union** also encourages member States to "cooperate to develop maintenance and repair capacities for submarine cable infrastructures".[241] The European Commission's 2025 Action Plan on Cable Security advances this intent, outlining key steps it will take in the short and medium term to ensure resilience in this area. In the immediate and short term, it proposes facilitating the contracting of repair services already available on the market through an existing Union Civil Protection Mechanism. It also discusses availing of modular repair equipment capacity as a kind of plug-and-play option. And it suggests stockpiling essential material and equipment. In the medium term and to prepare for potential systemic failures, it proposes supporting "the acquisition or contracting of additional repair and deployment vessels" for specific maritime basins, prioritizing the Baltic/North, that could be managed through regional framework agreements, a pilot of which could be tested in the Baltic Sea with relevant private sector actors. [242] Also in the medium term, the Action Plan proposes the establishment of a multi-purpose Cable Vessels Reserve Fleet to be used in emergency situations for repairing cables (optical fibre and electric) connecting Union territories, the funding for which could be drawn from existing funds, including the Connecting Europe Facility.[243] Moving forward on these actions will require deep engagement with the cable maintenance/repair industry, which itself is undertaking a study of marine maintenance for submarine cables to assess how the projected surge in new subsea cable deployments will impact maintenance needs and regional resources.[244]

For governments, understanding how the current repair ecosystem works can help to confirm factors already identified by industry that may delay repair and recovery efforts (e.g., lengthy permitting processes, backlogs of repairs), or inform ongoing discussions,

---

237 Kavanagh (2023), p.22

238 US Code (2021), Ch.532, Cable Security Fleet, § 53201, (1).

239 Ibid. § 53201- § 53205.

240 Brock (2023); Lartigue (2024).

241 European Commission (2024a), p. 5 para. 22.

242 European Commission (2025), Section 4.2, p. 13.

243 Ibid. p.14.

244 The study, supported by SubOptics Limited, is authored by Telegeography and Infra-Analytics. The results will be presented at the SubOptics conference in Lisbon in June 2025.

and, eventually, decisions on regulatory development/reform, government investment in cable maintenance and repair capabilities, and other measures that can strengthen the restorative capacities of subsea cable systems. This can include a consideration of their own connectivity needs and objectives, the availability of maintenance and repair vessels under existing maintenance arrangements[245] (figures 4 and 5 below) or regulatory issues. It can also include consideration of changes to the ecosystem that might affect the availability of vessels in the event of outages, for example SubCom's shift from maintenance work to installation, or perceived actions by hyperscalers to reduce costs, even when "margins are thin and contracts are short-term", in turn a disincentive for investing in new vessels which can cost up to USD 100 million.[246]

Systematic data gathering on cable repairs can also inform such decisions. As of today, most such data gathering on cable repairs tends to be collated by industry bodies (e.g., ICPC) or commercial entities (e.g., OceanIQ). For governments, working with industry to understand these existing data sets and their opportunities and limitations is important as they can provide a basis for investment decisions in the event of market failure.

One such data set is the **Global Cable Repair Data Analysis**, updated and presented at the ICPC's annual plenary meeting since 2011 and drawn from data provided to the ICPC by marine maintenance providers (cable maintenance zones and private maintenance agreements). Taking a traditional engineering approach, the analysis is centred on **the mean time to commence a repair effort**. Key data points used to assess the mean time to commence repair include interval times between notification of the incident (ideally a vessel would sail within 24 hours of notification); and arrival at the repair area, calculated as per distance to arrival, the jurisdiction (State) and the maritime area (territorial waters or EEZ) within which the cable lies.[247] Data analysis is then divided into subsets by zone and jurisdiction, and within each subset, a calculation is made to determine trends.

---

245 Through maintenance agreements, cable owners pool and share repair and maintenance capacities. There are two types of maintenance agreements: agreements based on geographical zones and private maintenance agreements on an ad hoc basis. In the first case, the cable owners organize themselves to sign a cable maintenance agreement based on geographical zones. In the case of private maintenance agreements, the owners of maintenance ships propose a maintenance service for individual cables; for more, see Agarwal (2024).

246 Dzieza (2024).

247 Palmer-Felgate et al. (2013).

FIGURE 4.

Cable zone maintenance agreements based on geographical zones.[248]

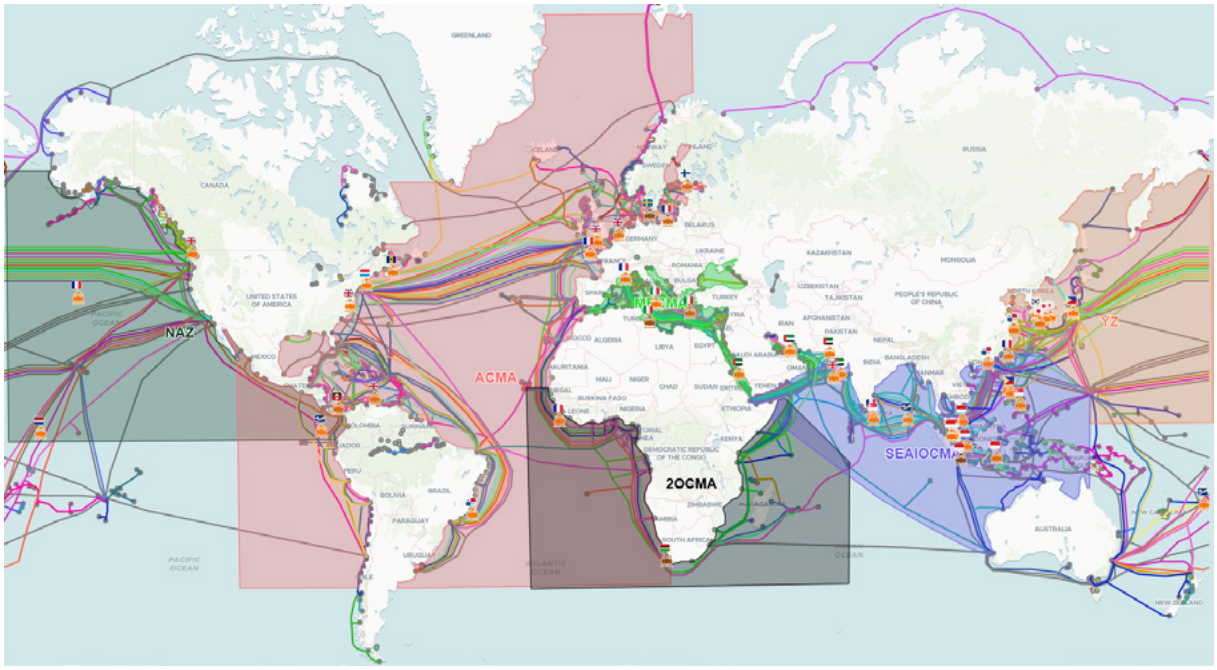
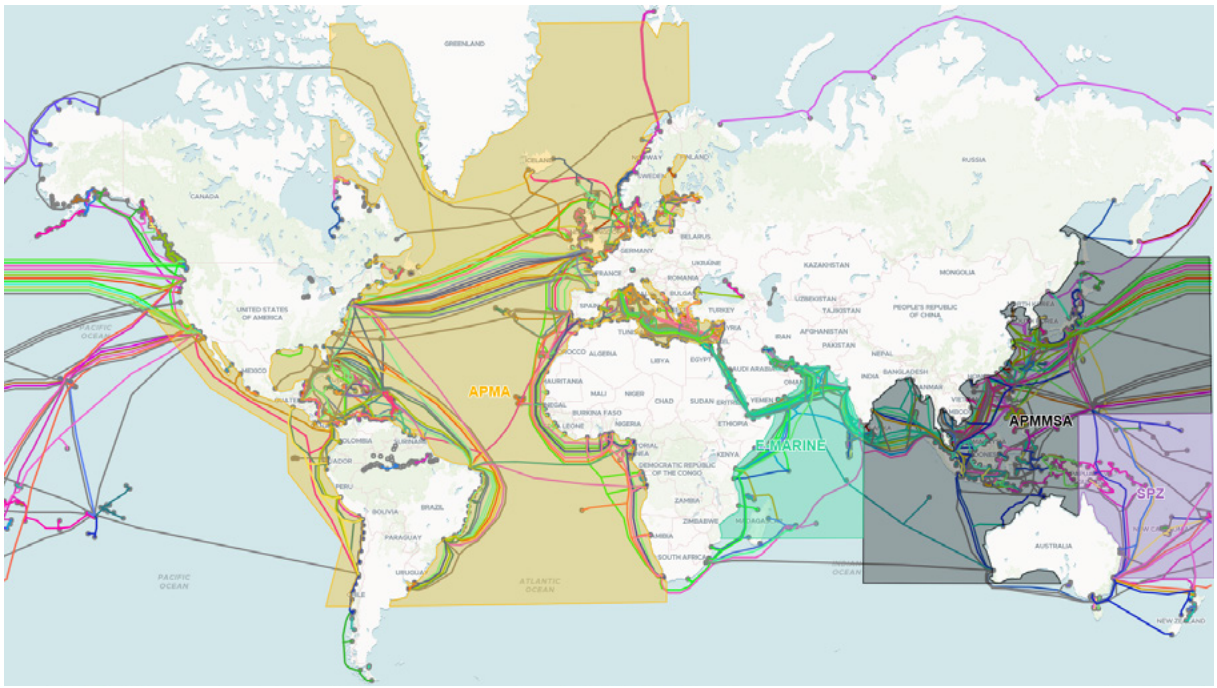


FIGURE 5.

Cable zone maintenance agreements based on private maintenance agreements.[249]



248 Figure by the authors, with cable data from TeleGeography (2024) and zone data from SubTel Forum (2022).

249 Ibid.

According to the analysis, several factors can impact the time it takes to commence a repair across the different cable maintenance zones. These can include weather conditions, geological events, permit requirements, transits, availability of vessel, crew and spares, and security and health requirements, all of which can manifest differently across maintenance zones.[250] Consider permitting requirements: some jurisdictions that experience one or more cable faults per year on average may have lengthier repair times due to post facto permitting requirements, in that they may require operators to seek a permit after an incident has occurred, or may impose cabotage restrictions. Others with a similar average may experience shorter times to repair due to an ex ante authorization system, for instance, only requiring notification once the repair is underway (**Belgium, France, Netherlands, South Africa, United Kingdom**).[251] As noted in the previous section, **China** relaxes its cabotage restrictions if a repair is urgently required on its continental shelf and as long as its sovereignty and jurisdiction are respected. Coordination between the maintenance provider, relevant government authorities and customers can also help accelerate repair efforts, as was the case with the C-Lion1, the high-capacity cable connecting Finland and Germany that was cut in November 2024.[252] So can sheer chance, as evidenced in the **Shetland Islands** incidents in 2022, where the fact that a repair ship was already in the vicinity contributed to accelerating the repair effort.[253]

As discussed, earthquake or flood resulting in landslides or turbidity currents can result in several cable outages in the same area, posing serious problems for the repair effort (**Taiwan**, 2006; **Japan**, 2011; **Tonga**, 2022; **Viet Nam**, 2023; **West Africa**, 2024). Many of these multi-cable events can have second and third order impacts that cause delays. For instance, in addition to severing seven of **Japan**'s 12 trans-Pacific cables, the 2011 earthquake and ensuing tsunami also caused a major nuclear accident at the Fukushima power plant. This meant that specialized equipment and gear as well as chemical weapons experts were needed to scan the water for radiation before the massive repair effort could commence.[254] Other external factors can create delays, as is clearly evident in conflict settings. As an example, in 2024 a combination of live fire, ongoing conflicts in the region, geopolitics, as well as sanction regimes and related legal conundrums significantly delayed the repair effort in the **Red Sea**.[255]

The results of the **Global Cable Repair Data Analysis** are important from a resilience perspective. For instance, according to the latest update of the global data, in 2023 there were reportedly some 206 repairs (up from 184 in 2022) within 136 different coastal jurisdictions, 54 per cent of which occurred in EEZs, 48 per cent in territorial waters, and 2 per cent in the high seas beyond the 200-mile limit. The average **notified-to-departure time** was 21 days; the average **transit time**, 7.5 days, while the longest repair delay was 947 days. As for **fault causes**, in 2023, 13 per cent of these faults were caused by geological events, abrasion and plant failure. The remainder were the result of what industry refers to as 'external

250 Palmer-Felgate et al. (2013); Dzieza (2024).

251 Palmer-Felgate (2024).

252 The cut followed that of the BCS East-West Interlink cable connecting Sweden and Lithuania.

253 Scottish Government (2023).

254 Dzieza (2024).

255 Interviews, April-October 2024; Valentia Island Symposium Proceedings Report (forthcoming).

aggression', meaning any damage caused by force.[256] The **types of fault** resulting from these were almost equal between an electrical fault (shunt only) and optical failure (loss of service).[257] At the same time, the global repair response time in 2023 more than doubled. The reason for these delays were due in part to regulatory requirements (e.g., vessel importation, bond provision, cabotage, operational permits, security clearances or sanctions compliance). Delays may also be due to a mix of factors such as repair backlogs, inclement weather, dearth of supplies, severity of the disruption (shunt fault with limited impact on traffic vs. full loss of service), in addition to or combined with any or several of the aforementioned regulatory issues. The **Asia-Pacific region** has tended to be the region with the longest mean time to commence repairs, in part due to long permitting processes (**China**, **Indonesia**), but also due to repair backlogs (**China**, **India**, **Viet Nam**), which in turn can lead to lesser vessel availability.[258] This can explain efforts by some governments in the region to promote investment in additional vessels either within existing maintenance agreements or as a sovereign capability (**India**, **Viet Nam**).[259]

In addition to considering the viability of investment in vessels per se, governments need to also assess the potential of new technologies for maintenance and repair – the engineering and other niche skills required to repair fibre-optic cables and crew the vessels, including under complex conditions at sea and taking into consideration existing workforce challenges.[260] Such investment decisions should also be assessed against different connectivity options (diversity of cables, providers, routes, international capacity, terrestrial fibre, local Internet exchanges) and other digital infrastructure (e.g., satellite connectivity) that can ensure business continuity during unforeseen events.

Finally, in most instances, repair ships should be able to conduct their operations as usual. However, in disputed areas or in situations of conflict, they may need to request or may be offered to be escorted by coast guards or navies. In some instances, an installation or repair operation may be delayed due to sanctions or other restrictions impeding them from entering a certain area. In each of these situations, significant back-channelling to secure access, including for an escort or exemptions from sanctions, is key. Several States are beginning to take these issues seriously.[261] A deeper dive into the legal, diplomatic, operational and financial implications of operating under such conditions would be a useful contribution to ongoing discussions.

---

256 Palmer-Felgate (2024).

257 An electrical fault occurs when the insulation of a subsea cable is damaged, exposing the metallic core to seawater and causing a short circuit. While data transmission may not be immediately interrupted, prompt repairs are necessary to prevent further issues. In contrast, an optical failure happens when fibre damage disrupts data transmission, leading to service loss that requires repairs to restore connectivity.

258 Palmer-Felgate et al. (2013); Palmer-Felgate (2024).

259 Ibid.

260 Interviews, April-October, 2024.

261 Interviews, April-October 2024.

4.3. Adaptive Capacities

Adaptive capacities refer to the ability of a system to adjust, respond to changing conditions, and evolve after a disruption. It also means implementing changes to current practices or policies, and to learn from disruptions, for example, through revising plans, modifying procedures, and introducing new tools, technologies, and training exercises – that is, everything that is needed to improve before the next crisis hits. Governments contribute to enhancing the adaptive capacities of subsea cable systems through a range of measures, including by learning from incidents, ensuring that regulatory processes remain dynamic, exchanging national views on international law and addressing identified gaps, and through diplomatic action and international cooperation.

4.3.1. Learning from incidents

As has been discussed, many States and regional organizations are beginning to integrate subsea cable system-related issues into more long-term resilience or emergency planning. Learning from incidents and from regularly conducted exercises are important ways to assess the need for policy or regulatory change, for identifying investment needs, for clearly identifying and reconfirming roles and responsibilities of public and private actors in national preparedness and crisis response, and for relevant communications to the public in the event of an incident. There are sufficient lessons from recent cable damage incidents to learn from, exchange best practices on, and further fine-tune preparedness and crisis management processes and procedures. Where appropriate, involving relevant industry players in these efforts is essential, not least since in addition to operating the systems, they will be the first responders in most cases, and are responsible for ensuring business continuity.

Recent incidents have aptly demonstrated the importance of having in place **clear and timely internal modes of reporting and communicating** on an incident and **clearly defined roles and responsibilities** for relevant agencies and cable operators at the local level, all the way through to the relevant regional and national authorities. Moreover, recent incidents demonstrate the need to ensure that government authorities at the highest levels are aware of these procedures and how they work in practice. Several recent incidents also demonstrate the importance of effective **communications** when incidents occur, and of **reassuring populations** in the event of partial or complete loss of service that repairs are underway, and that connectivity will be shortly reinstated. When relevant, cable operators or service providers notify their clients when an incident is serious enough, and when service has been restored. Governments, too, are beginning to take on this task, as part of general civil protection and resilience efforts. For instance, following the March 2024 subsea cable disruptions off the coast of West Africa, **Ghana's National Communications Authority** put out seven advisories on the disruption, from the moment of the disruption until the repair effort had been completed some two months later.[262] Meanwhile, as part of their broader societal resilience actions, some States are making a concerted effort to ensure that their societies are prepared for prolonged disruption of communications, be it caused by natural events or by hostile State actions (**Pacific Island States**, **Finland**, **Iceland**, **Norway**, **Sweden**).

Responsibility for an incident may take time to ascertain and, for a number of reasons, may

[262] See National Communications Authority Ghana (2024).

never be publicly attributed. Nonetheless, as in other areas, for governments rapid communications on an incident, regardless of its cause, are imperative in the current environment, especially to buffer against mis- and disinformation and irresponsible statements or reporting. For instance, in the Shetlands case (and others since), media outlets were quick to assume that the disruption resulted from the actions of a hostile State actor, drawing conclusions from the fact that the incident occurred the same year as the Nord Stream pipeline and Svalbard cable incidents, yet paid limited heed to the scores of cable incidents that have occurred in the same area over the preceding decade. While the relevant authorities quickly confirmed among themselves that the incident was caused by a fishing vessel, they were criticized for failing to publicly communicate what they knew and for allowing such speculation.[263] Indeed, media and think-tank reports continued to describe the incident as a result of hostile State action months after the incident. More responsible reporting would have looked at cable damage trends in the specific area, which would have immediately pointed to trawling as the likely cause of damage, even if sabotage could not immediately be ruled out. Similarly, in 2024, the **Red Sea** outages led to significant speculation about the incident, with commentators quickly latching on to the streams of misinformation and disinformation flowing on social media. Closer collaboration behind the scenes, however, allowed for light to be shed on the more likely cause of the incident, even if it took longer for such news to take root on social media.[264] In the more recent **Baltic Sea** cases, speculation of sabotage abounded even before official investigations and industry repair efforts were properly underway, influenced in large part by the broader geopolitical context.[265] Again, while sabotage may well have been the cause of some of these incidents, in situations of heightened tensions like these, responsible communications (and reporting) is imperative.

Some of these incidents also point to the **age-old problems confronting seabed users** that can become enmeshed in domestic and global politics. In the Shetland Islands case, the cable incident became an item of debate in the Scottish Parliament and opened a discussion on competing seabed uses, and on potential yet complex solutions such as the establishment of designated cable corridors (as noted this can create further headaches for governments, due to the concentration of risk in one specific area). These and other such incidents can shed light on underlying issues requiring attention, such as updating legislation, streamlining regulation, ensuring effective accountability for cable damage, regulating and policing the use of automated identification systems and ensuring easier access to vessel monitoring systems, promoting, adopting and implementing effective measures directed at fishing and anchoring risks, and advancing discussions on marine spatial planning. Advancing these issues would help to mitigate the most common forms of cable damage, thus allowing industry to keep data flowing and governments to focus on strategic threats.

Lastly, governments should also use **national preparedness exercises** and drills to inform **emergency preparedness and crisis response planning**. For example, **Portugal** hosted a submarine cable security exercise in Lisbon in October 2024 to enhance awareness, training, and cooperation among key stakeholders. Participating entities included “a wide range of companies, including operators and manufacturers, other regulators, various

263 Marter (2023).

264 Interviews, April-October 2024.

265 Interviews, April-October 2024; Valentia Island Symposium, October 2024.

public, civil and military bodies, as well as several municipalities."[266] Ensuring such exercises – and lessons learned from them – are informed by the expertise of relevant operators and others such as international law and other thematic experts, and that they are joined up with relevant crisis management and decision-making processes, are equally key.[267]

4.3.2. Regulation

Today more than ever, subsea cable-related regulation needs to be nimble and dynamic, and harmonized as much as possible between connected States. Governments need to ensure that submarine cable-related regulation is appropriately balanced with other regulatory frameworks, and further that it is adaptive to changing circumstances. This is particularly important where new cable ownership structures, marine spatial planning, national security, climate disaster preparedness and equities management are concerned. Having in place mechanisms that facilitate coordination across regulators within and across borders and that foster appropriate means of engagement with industry and academia can help to identify those issues that require urgent attention and ensure that regulatory decisions have a strong evidence base.

Dedicated platforms, too, can be useful for informing policy or regulatory directions where subsea cable security and resilience are concerned. For instance, in the context of the **European Union**, the Body of European Regulators for Electronic Communications assists the European Commission and the National Regulatory Authorities in implementing the Union's regulatory framework for electronic communications. A June 2024 report by the Body of European Regulators highlights some of the challenges that national regulatory authorities are confronting, particularly where new subsea cable ownership structures are concerned, with major technology companies becoming the main players.[268] Such discussions are emerging at a time of growing concerns about over-dependence on big technology companies for everyday societal needs, over which there is limited democratic control.[269]

In southeast Asia, attempts have been made to take a regional approach to subsea cable-related issues. Examples include the **Council for Security Cooperation in the Asia Pacific** Memo on crisis management and contingency planning, currently being updated.[270] The **European Union** has convened an informal expert group to determine how best to implement its Recommendation on Secure and Resilient Submarine Cable Infrastructures. The envisioned mandate of the expert group is broad. It entails annually mapping submarine cable infrastructures across the Union as well as reviewing national approaches to risk assessment to identify missing information and proposing measures to complete these gaps, thereby supporting the creation of a comprehensive Union-wide risk assessment that – ideally – is to be reviewed annually. It is also tasked with drafting the initial list of 'Cable Projects of European Interest' that meet the criteria outlined in the Recommendation. Additionally, the expert group will be responsible for exploring technical solutions to detect and deter threats to submarine cables, particularly those resulting from EU-funded projects, as

266 Autoridade Nacional de Comunicações (2024).

267 Dombrowski and Reich (2024).

268 BEREC (2024a).

269 Ministry of Digital Affairs, Denmark (2024).

270 Council for Security Cooperation in the Asia Pacific (2014).

well as maintenance and repair capacities.[271] For now, the expert group appears principally to involve only government representatives, but public tenders and consultations with industry and relevant associations are underway, which may well help to avert further complexity than already exists.[272]

4.3.3. International law

International law plays a crucial role in enhancing the resilience capacities of subsea cable systems by establishing a legal framework that promotes protection, cooperation, and accountability. Yet, it is the least adaptive of all measures required to protect the infrastructure. As discussed in our 2023 report, concerns that the international law governing subsea cables may no longer be fit for purpose have been floated for several decades.[273] Given the uptick in incidents affecting subsea telecommunication cable systems, governments and other actors continue to invest resources in understanding potential gaps in existing international law. This is a long-term process, but one that may eventually bear fruit. For instance, reflecting growing concerns of possible sabotage of subsea cable systems, in 2024 the **International Law Association Committee on Submarine Cables and Pipelines** under International Law produced its Third Interim Report, focusing "on the international law that governs the measures that States can take in response to intentional acts of damage to submarine cables and pipelines committed by States and non-State actors in peacetime".[274] The preliminary conclusions of that report are important and merit consideration as States themselves consider how best to respond to such acts. Indeed, the concluding section notes that States can take a range of measures in response to intentional damage to submarine cables and pipelines. It also notes, however, that "the ambit of some of these measures are uncertain and require further discussion and clarity".[275] In addition to the work of the International Law Association, legal scholars across the globe are producing scores of articles on different issues relevant to subsea cables in crisis and conflict, including with regard to imposing costs on hostile actors for intentional cable damage, or on the rights and obligations of private corporations operating in contested waters, which under UNCLOS, are not conferred on them directly.[276] At national level, parliamentary hearings focusing on the law of the sea have included questions relevant to subsea cable protection and on whether the current regime is fit for purpose.[277] Each of these identify gaps and serve as important guidance or input to States as they review their own national approaches to addressing some of these gaps.

---

271 European Commission (2024a), p. 3.

272 Submarine Cable Infrastructure Expert Group (2024).

273 Kavanagh (2023), pp.24-28.

274 Established by the International Law Association Executive Council in November 2018, the Committee continues to produce its interim reports, having acknowledged that the current international legal regime governing submarine cables and pipelines established by UNCLOS (and other conventions) "may not adequately address the myriad of challenges that States, and entities engaged in cable and pipeline activities, currently face in the development of policies relating to all aspects of submarine cables and pipelines"; International Law Association (2024), p. 3. Already in 2014, the Handbook of Law and Policy on Submarine Cables dedicated a chapter to intentional damage; see Burnett, Davenport and Beckman (2013), chp. 12.

275 International Law Association (2024), Section VI, Preliminary Conclusions, p. 55. para.182.

276 See Tammikko (2024); Davenport (2024); Ryan (2024); McLaughlin, Paige, and Guilfoyle (2022);

277 UK Parliament 2025.

4.3.4. Subsea cables in foreign policy

Many governments are increasing their foreign policy action on subsea cable systems.[278] **China** was a forerunner where integrating subsea cables into foreign policy objectives is concerned.[279] The **United States** has recently geared up action in this area. For example, its 2024 International Cyberspace and Digital Policy Strategy includes a dedicated line of effort on enhancing the security and resilience of undersea cables which discusses the CABLES programme, implemented since 2021 in the East Asia-Pacific region and strongly focused on promoting its policy of trusted suppliers.[280] The Strategy's 'line of effort' also mentions joint investments alongside **Australia** and **Japan** in Micronesia totalling USD 21 million, as well as a new commitment in 2023 to invest jointly with **Australia** some USD 65 million to fund future undersea cable connectivity for Pacific Island countries so as to enable them to "access global markets and meet their regional connectivity goals".[281]

Australia has also established a Cable Connectivity and Resilience Centre with the aim of providing "demand-driven technical assistance, commissioning research and analysis and convening dialogues and knowledge-sharing activities".[282] Implemented across **South Asia**, **South-East Asia** and **the Pacific**, many of these activities are implemented with other strategic partners such as the **United States**, or through more security focused groupings such as the **AUKUS** partnership and the **Quadrilateral Security Dialogue**.[283] For its part, the **European Union** has proposed to advance cable diplomacy within its Action Plan on Cable Security. Included under the deterrence pillar of the Action Plan, this will involve promoting the principles of the Cable Security Toolbox with partner States, enhancing the exchange of information on incidents with partners in the Indo-Pacific experiencing similar challenges, and raising cable and security issues at the highest levels in multilateral forums such as the United Nations and in relevant security and defence dialogues and defence partnerships.[284]

Some of these outward-looking efforts are questioned for being driven by the national security and trade interests of the States providing the investment or assistance, and for sometimes being detached from their own national efforts to enhance resilience, which may at times lag behind those States they are hoping to assist. This should be acknowledged and these actions, like those of others, should be scrutinized. At the same time, this new form of cable diplomacy does provide connectivity often where connectivity was heretofore non-existent or unreliable. It is leading to a greater number of exchanges within and across regions on national policy, regulation, incident reporting and response, and on other good practices relevant to subsea cable infrastructure protection, which is helping to shed light and advance discussions on identified gaps and regulatory bottlenecks. Assessing the effectiveness of these efforts in terms of

278 Bueger, Liebetrau, and Franken (2022).

279 Aluf (2023), p. 3.

280 US Department of State (2024b).

281 Prime Minister of Australia (2023).

282 Department of Foreign Affairs and Trade, Australia (2024).

283 Ibid.

284 European Commission (2025), p.16-17.

their contribution to resilience goals will be an important next step in this emerging field.[285]

Across regions, industry associations are also investing significant resources in awareness raising and in engagement with national governments, regional governmental structures such as the **Association of Southeast Asian Nations** and the **European Union**, and with regional security organizations such as **NATO**. These engagements include exchanges on national policy and regulation, and on international law matters, and, more recently, on maritime safety and maritime domain awareness, or cyber and supply chain security issues.[286] African States are calling for more of these kinds of cooperative actions, notably on maintenance and repair, both within existing continental and regional structures such as the **African Union** and the **Economic Community of West African States** and through the establishment of new ones such as the aforementioned International Advisory Body jointly led by the ITU and ICPC.[287] Meanwhile, in Latin America, **Brazil** for example is investing heavily in partnerships to raise awareness of cable security and resilience within government and among potential newcomers to the industry. It has also established its own national Cable Protection Committee.[288]

4.3.5. The role of technology

Technology plays an important role in ensuring the resilience capacities of subsea cable systems. Governments are paying special attention to sensor technologies for deterrence and defence. These include the various kinds of sensor data being developed to support better network resilience and better maritime situational awareness. Currently, the cable industry already sits on vast amounts of data on their cables and the seafloor surroundings, be it from desk studies, pre-surveys, or laying and maintenance activities. The performance of active cables is continuously monitored through the network management system in the landing stations or remotely. Operators are instantly alerted in the event of shunt faults or loss of service. The type of outage and distance to it is quickly identified through standard procedures.

Governments willing to invest can use multiple sources of information to monitor activity around cables above, on and below their waters. The maritime situational picture often relies on automatic identification services, sometimes supplemented by data from vessel monitoring systems. Increasingly, optical and synthetic aperture radar satellite technologies feed into the maritime surface information landscape. Asset management and monitoring systems are mostly used by maritime energy infrastructure operators, although some specialized companies have recently extended their commercial services to data cables. Government patrols over cable infrastructures can add another layer of information. Relevant capabilities vary between vessels that are surface or subsurface, crewed or uncrewed, and remotely controlled or autonomous. Suitability depends on the maritime context, technological capacity and aims of the patrol. For example, large-scale surface data traffic can best be gathered by naval surface vessels, while uncrewed vessels equipped with optical sensors can be instrumental for explosives detection on cable sections where suspicious movements are detected. For example,

---

285 Alongside cable diplomacy, collective resilience efforts between independent States have been investigated in regions such as the Caribbean. A strategic network resilience approach was used to assess such efforts. Starosielski et al. (2025).

286 Interviews April-October 2024.

287 International Telecommunication Union (2024).

288 Interview, April 2024 and written communication with Brazilian expert, December 2024.

according to a parliamentary hearing, the **German Navy** is opting for "crewed systems if necessary, uncrewed systems if possible" to fulfil the task of maritime surveillance and deterrence.[289] Data generated by these and other sources can ideally be fused into a whole operational picture. For example, the **Irish Naval Service**'s Recognised Maritime Picture includes video footage of ports additional to data from automatic identification systems, vessel monitoring systems, radio traffic and intelligence analysis, "as well as incidental or planned Air Corps observation reports and radar tracks".[290]

Another foreseeable technological shift is the increasing use of cables as sensors, such as through the Science Monitoring and Reliable Telecommunications (SMART) cable initiative.[291] For example, **Portugal** is leveraging the technology in the New CAM Ring project to establish sensor-equipped connections between the mainland, Madeira, and the Azores.[292] Distributed acoustic sensing (DAS) is a fast-developing alternative. Here, vibrations on the cable are measured through changes in light reflections within a fibre.[293] While SMART cables have to be planned as such from the project start, it is possible to retrofit existing systems for DAS from the landing station to the first repeater, usually 60-80 km offshore. When DAS is included from the outset, the possible measurement distance can go beyond the first repeaters in shallow waters. For example, the Medusa Project, a planned subsea cable connecting 11 countries in the Mediterranean Sea, is envisioned to have distributed acoustic sensing technology deployed in eight of its landings in EU States (**Portugal**, **Spain**, **France**, **Italy**, **Greece**, **Cyprus**).[294] Other sensor technologies such as the **state of polarization** and **optical interferometry** offer the potential to use the full length of a cable and can be retrofitted to fibre-optic cables. However, they are not as effective at detecting small-scale events along the cable.[295] In the long term, emerging technologies such as quantum sensing may also bring improvements to the surface and subsea situational picture, potentially leading to much more transparent oceans.

For obvious reasons, cable sensor data is of much interest to both operators and governments, yet it comes with two major caveats. First, the installation of sensors and the storage and analysis of the vast amounts of sensor data are costly. Scaling effects may however mitigate the resource question. Second, the data generated provides the potential to monitor the water column. It is, therefore, perceived as sensitive by some actors – foremost governments that have undersea capabilities, although the technology itself can be leveraged to resolve this issue. More complex are concerns that such uses of subsea cables may change their character from a mostly civilian infrastructure to one creating data for military use, which may lead to changes in government oversight,

289 Deutscher Bundestag (n.d.).

290 McCabe and Flynn (2024), p. 12.

291 International Telecommunication Union (2012).

292 Bernardino (2024).

293 Waagaard et al. (2022).

294 European Commission (2022).

295 State of polarization analyses changes in the polarized light transmitted through telecommunications cables, offering medium environmental sensitivity and a range spanning thousands of kilometres. It can detect and locate disturbances such as earthquakes with a spatial resolution defined by repeater distances, without requiring hardware modifications. Optical interferometry employs highly stable lasers to detect phase changes in light caused by environmental factors like pressure or cable movements. This method is highly sensitive, operates over similar ranges, and enables precise detection of signals between cable repeaters; see Clare (2024) for more detail.

new licensing regimes, and strict data-sharing or reporting arrangements. In times of conflict, sensor-equipped cables may also suffer from lower thresholds of proportionality in determining their eligibility as lawful targets.

Lastly, as noted on several occasions across this report, bringing these data points together with other data sources and intelligence for situational awareness and to inform decision-making is a process that many governments are only beginning to grapple with. The **European Union**'s proposed Integrated Surveillance Mechanism for Submarine Cables is an interesting start. A voluntary mechanism, it aims to link and fuse data gathered via different systems and sources to provide timely and accurate situational awareness for early warning and to enhance attribution capacity. Funding and political will permitting, the Baltic Sea may well become the first test bed for such a regional surveillance hub. [296] The initiative will undoubtedly provide useful lessons on collaboration and information-sharing between the governments involved and the owners and operators of the very systems the initiative is setting out to protect. Meanwhile, more effort needs to be placed on how other technologies such as quantum communication, encryption and sensing technologies will shift how we think about security and resilience of these systems in the future.

4.3.6. The role of academia

Academia has historically played a role in advancing thinking and knowledge development around issues emerging on the policy agenda. Research institutes across the globe are developing research streams on different aspects of subsea telecommunications cable security and resilience, and on critical undersea infrastructure or digital infrastructure protection more broadly. These research streams are often disconnected from each other and from government policy and industry action. This is not necessarily a negative, but there are some instances when cross-disciplinary research and engagement involving multiple stakeholders can have enormous policy value, helping to raise awareness, reach common understandings, identify research and policy gaps and much else that contributes to resilient systems. Dedicated academic programmes play an important role in this regard and are already under development.[297] Other instances of such kinds of knowledge-based engagement are already taking place and should be further supported.[298]

---

296 European Commission (2025), p. 9–10.

297 Programmes such as the Certificate in Global Digital Infrastructure in development at the University of California, Berkeley in the United States --which has a unit specifically on subsea cable protection, security, and resilience, or the second level Master's degree in Digital Subsea Infrastructures, currently in development at the University of Genoa in Italy, are a case in point. Starosielski et al. (2025); interviews April-October 2025.

298 Recent examples include the October 2024 Inaugural Valentia Island Symposium on Subsea Cable Security and Resilience held in Co. Kerry, Ireland; the launch that same month of the Portugal-based Observatory of Digital Ecosystems and Infrastructures; different NATO Science for Peace and Security Programme-funded workshops; EU Horizon tenders; and loose networks of academics such as the Subsea Cable Academic and Arts Network (SCAAN).

5. Concluding Remarks

Undoubtedly, subsea telecommunications cables are on the radar (and, in some cases, the sonar) of governments across the globe. While the reasons for this attention differ across countries and regions, a point of commonality is our ever-expanding dependence on these systems. Most States designate or qualify the infrastructure or elements thereof as critical or vital, the security and resilience of which is essential. Through the lens of three core resilience capacities – absorptive, restorative and adaptive – this report examined what a criticality designation means in policy and practice.

For now, most government actions fall under the rubric of **adaptive capacities**. They include using regulation to protect these systems across a number of areas (redundancy, spatial separation, charting of cables, cable damage penalties, streamlining permitting and licensing for installation and repair). Regulation also plays a role in contributing to the **restorative capacities** of subsea cable systems. We have highlighted actions that some States are taking to ensure that cable ships have expedited access for repair to ensure the systems are restored in a timely manner. Industry bodies such as the ICPC have already recommended such regulatory action as resilience best practice and it figures strongly in recent inter-governmental recommendations, statements and declarations. We also include more security-oriented regulations – cybersecurity and supply chain security in particular – since they also aim to protect these systems. We caution, however, that some such measures require constant review and adaptation so as not to undermine the resilience of the systems and expose States to new vulnerabilities.

Most emergency preparedness and crisis management actions also fall under the **absorptive capacity** rubric. It is here that much innovation is happening at government level, with new coordination structures, reporting requirements and cooperative arrangements being established and new capabilities deployed either to protect the systems or deter potential malicious activity. Hence, when an incident occurs, these different mechanisms and procedures can be activated, thus contributing to the systems' **restorative capacities** even if on most occasions the response and recovery effort will remain the responsibility of the cable systems' owners and operators. We suggest that this is one area that requires more attention in the current context. Under the **restorative capacity** rubric, we also saw that some States are considering whether to invest in maintenance and repair capabilities for both resilience and security purposes. Understanding the many underlying issues that may delay mean time to repair is critical to informing such investment decisions. Here again, we see the resilience cycle at play.

Recent subsea cable incidents are providing ample lessons for States to fine-tune their response mechanisms and to clarify roles and responsibilities across government and industry in different situations (peacetime, crisis or conflict). We have included this learning process under the rubric of **adaptive capacities** which can also entail regular reviews and fine-tuning of regulation, of crisis management protocols, of deterrence strategies and operational rules of engagement or of industry engagement mechanisms. It might also include addressing gaps in international law, establishing new forms of diplomatic engagement, or testing how extant and emerging technologies can contribute to resilience and

security. Such learning should ideally feed back into the **resilience cycle**, thus contributing to the strengthening of the systems' other capacities.

These and the many other efforts we observed vary significantly across States in terms of their implementation and maturity. Indeed, the practical differences that occur as a result of a CI designation vary significantly from country to country. These differences can be particularly problematic for connected countries. For instance, from a national preparedness perspective, it makes limited sense if only two out of three connected States designate points of contact at policy and operational levels or if only two out of the three have streamlined and harmonized their regulations.

Hence our recommendations. Principal among these is the recommendation that States develop national security and resilience frameworks that contribute to the three core resilience capacities of subsea cable systems – absorptive, restorative and adaptive – in order to prepare for, respond to, and recover and learn from unexpected or changed circumstances. These are fundamental features of the resilience cycle and are key drivers of societal resilience and national security. Critical to the effectiveness of such frameworks are the cross-cutting issues we note – international law, guiding principles, equities management and, importantly, the engagement of players in the subsea cable industry ecosystem that design, install and operate the cables and that are ultimately responsible for their maintenance, recovery and repair.

Submarine cable inspection vessel.
Credit: Korn Srirawan / Shutterstock.

References

Agarwal, Soham. 2024. “Enhancing Capacity-of and Capabilities-in Repair of Submarine Communication Cables through International Cooperation.” *National Maritime Foundation*, May 14, 2024. https://maritimeindia.org/enhancing-capacity-of-and-capabilities-in-repair-of-submarine-communication-cables-through-international-cooperation

Agência Nacional de Telecomunicações Brasil. 2023. “Anatel debate importância dos cabos submarinos [Anatel Debates Importance of Submarine Cables].” *Ministério Das Comunicações*, 27 September 27, 2023. https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-debate-importancia-dos-cabos-submarinos

Allam, Hannah. 2008. “Cut Middle East Internet Cables Remain a Mystery.” *The Seattle Times*, 6 February 2008. https://web.archive.org/web/20090404002643/http://seattletimes.nwsource.com/html/nationworld/2004166752_internet06.html

Aluf, Dale. 2023. “China’s Subsea-Cable Power Play in the Middle East and North Africa.” Issue Brief. Atlantic Council. https://www.jstor.org/stable/resrep51431

ANACOM. 2020. “Working group on the future of submarine cables for CAM communications makes 12 recommendations”, https://www.anacom.pt/render.jsp?contentId=1499946

APEC Policy Support Unit. 2012. “Economic Impact of Submarine Cable Disruptions.” Asia-Pacific Economic Cooperation Secretariat. https://www.apec.org/docs/default-source/publications/2013/2/economic-impact-of-submarine-cable-disruptions/2013_psu_-submarine-cables.pdf

Asian Development Bank. n.d. “Financial and Economic Analyses.” Asian Development Bank. Accessed December 2, 2024. https://www.adb.org/sites/default/files/linked-documents/44172-022-ton-efa.pdf

Australia Department of Foreign Affairs and Trade (n/d). “Cable Connectivity and Resilience Centre”. https://www.dfat.gov.au/international-relations/regional-architecture/quad/cable-connectivity-and-resilience-centre

Autoridade Nacional de Comunicações. 2019. “Regulation No. 303/2019: Regulation on the Security and Integrity of Electronic Communications Networks and Services.” *Diário da República*, no. 64 (Serie II-Part E), April 1, 2019. https://www.anacom.pt/render.jsp?contentId=1469920&languageId=1

———. 2023. “ANACOM present at REPMUS23” October 10, 2023. https://www.anacom.pt/render.jsp?contentId=1756381

———. 2024. “ANACOM Promotes Submarine Cable Security Exercise to Strengthen the Security and Resilience of the Sector.” October 24, 2024. https://anacom.pt/render.jsp?contentId=1797895

Bafoutsou, Georgia, Maria Papaphilippou, and Marnix Dekker. 2023. “Subsea Cables - What is at Stake?” European Union Agency for Cybersecurity (ENISA), July 2023. https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf

BEREC. 2024a. “BEREC Report on the General Authorisation and Related Frameworks for International Submarine Connectivity.” BoR (24) 85. https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-general-authorisation-and-related-frameworks-for-international-submarine-connectivity

———. 2024b. “BEREC Vice-Chair Outlines Possible Legal Ramifications of New Global Connectivity Trends,” July 12, 2024. https://www.berec.europa.eu/en/news/latest-news/berec-vice-chair-outlines-possible-legal-ramifications-of-new-global-connectivity-trends

Bernardino, Luís. 2024. “Geostrategic Position of Portugal in the Global Submarine Cable Network. Challenges and Opportunities” *Eurodefense*, July 31, 2024. https://eurodefense.pt/wp-content/uploads/2024/08/20240731_Geostrategic-position-of-Portugal-in-the-global-submarine-cable-network.pdf

Blanchard, Ben, and Yimou Lee. 2025. “Taiwan Coast Guard Says Investigation of Damaged Undersea Cable Stymied by Weather.” *Reuters*, January 7, 2025. https://www.reuters.com/world/asia-pacific/taiwan-coast-guard-says-investigation-damaged-undersea-cable-stymied-by-weather-2025-01-07

Bricheno, Lucy, Isobel Yeo, Michael Clare, James Hunt, Allan Griffiths, Lionel Carter, Peter J. Talling, et al. 2024. “The Diversity, Frequency and Severity of Natural Hazard Impacts on Subsea Telecommunications Networks.” *Earth-Science Reviews* 259 (December). https://doi.org/10.1016/j.earscirev.2024.104972

Brock, Joe. 2023. “Inside the subsea cable firm secretly helping America take on China’.” *Reuters*, July 06, 2023. https://www.reuters.com/investigates/special-report/us-china-tech-subcom/

Broeders, Dennis, and Camino Kavanagh. 2023. “Shades of Grey: Cyber Intelligence and (Inter)National Security.” Policy Brief. EU Cyber Direct. https://eucyberdirect.eu/research/shades-of-grey-cyber-intelligence-and-inter-national-security

Bueger, Christian, and Tobias Liebetrau. 2021. “Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network.” *Contemporary Security Policy* 42 (3): 391–413. https://doi.org/10.1080/13523260.2021.1907129

Bueger, Christian, Tobias Liebetrau, and Jonas Franken. 2022. “Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU.” In-Depth Analysis Requested by the SEDE sub-committee PE702557. European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Burdette, Lane. 2024. “What to Know about Submarine Cable Breaks.” *TeleGeography*, November 21, 2024. https://blog.telegeography.com/what-to-know-about-submarine-cable-breaks

Burnett, Douglas R., Robert Beckman, and Tara M. Davenport, eds. 2013. *Submarine Cables: The Handbook of Law and Policy*. Leiden, The Netherlands: Brill | Nijhoff. https://doi.org/10.1163/9789004260337

Carter L., Burnett D., Drew S., Marle G., Hagadorn L., Bartlett-McNeil D., and Irvine N. (2009). Submarine Cables and the Oceans – Connecting the World. UNEP-WCMC Biodiversity Series No. 31. ICPC/UNEP/UNEP-WCMC. http://www.iscpc.org/publications/icpc-unep_report.pdf

Caixiong, Zheng. 2024. “4条国际海缆被船锚拉断!广东海警侦破一起国际海缆损坏案 [Four International Sea Cables Were Pulled off by Ship Anchors! Guangdong Marine Police Solved an International Sea Cable Damage Case].” *Guangdong Bureau of China Daily*, January 13, 2024. https://gd.chinadaily.com.cn/a/202401/13/WS65a1ee51a310af3247ffbd06.html

Cho, Kenjiro, Cristel Pelsser, Randy Bush, and Youngjoon Won. 2011. “The Japan Earthquake: The Impact on Traffic and Routing Observed by a Local ISP.” In *Proceedings of the Special Workshop on Internet and Disasters*, 1–8. Tokyo: ACM. https://doi.org/10.1145/2079360.2079362

Clare, Mike. 2024. “Submarine Cable Protection and the Environment.” *International Cable Protection Committee* 8 (April). https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/?id=8

Collier, Stephen J., and Andrew Lakoff. 2008. “The Vulnerability of Vital Systems: How ‘Critical Infrastructure’ Became a Security Problem.” In *Securing “The Homeland”: Critical Infrastructure, Risk and (In)Security*, edited by Myriam Dunn Cavelty and Kristian Soby Kristensen. London; New York. https://stephenjcollier.com/wp-content/uploads/2012/07/collier_lakoff_vulnerability_2008.pdf

Council for Security Cooperation in the Asia Pacific. 2014. “Safety and Security of Vital Undersea Communications Infrastructure.” Memorandum CSCAP MEMORANDUM NO. 24. Council for Security Cooperation in the Asia Pacific (CSCAP). http://www.cscap.org/uploads/docs/Memorandums/CSCAP%20Memorandum%20No.24%20-%20Safety%20and%20Security%20of%20Vital%20Undersea.pdf

Creemers, Rogier, Samm Sacks, and Graham Webster. 2021. “Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021).” *DIGICHINA Standford University*, August 18, 2021. https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/

Communications Security, Reliability, and Interoperability Council. 2014. “Final Report – Protection of Submarine Cables through Spatial Separation.” https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf

Davenport, Tara. 2024. “Intentional Damage to Submarine Cable Systems by States,” Aegis Series Paper No. 2305, Hoover Institute, Stanford University, 1-24, https://cil.nus.edu.sg/publication/intentional-damage-to-submarine-cable-systems-by-states-by-tara-davenport/

Davenport, Tara. 2015. “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis.” *Catholic University Journal of Law and Technology* 24 (1): 57–109. https://scholarship.law.edu/jlt/vol24/iss1/4

Department of Environment, Climate and Communications. 2024. “The National Cyber Security Bill 2024 Heads of Bill,” September. https://assets.gov.ie/303962/aa59bc78-e82d-4e74-9e95-b05c0c5a83a1.pdf

Derouin, Sarah. 2017. “Benchmarks: November 18, 1929: Turbidity Currents Snap Trans-Atlantic Cables.” *Earth Magazine*, October 27, 2017. https://www.earthmagazine.org/article/benchmarks-november-18-1929-turbidity-currents-snap-trans-atlantic-cables/

Deutscher Bundestag. n.d. Ausschuss für Inneres und Heimat. *Beitrag Der Marine Zum Schutz Maritimer Kritischer Infrastruktur*. *Ausschussdrucksache 20(4)456 B*. Accessed December 20, 2024. https://www.bundestag.de/resource/blob/1010592/87fd1110fb83656e42823e11ccdedecf/20-4-456-B.pdf

Dludla, Nqobile. n.d. “Fibre Optic Cables Should Be Considered ‘Critical Infrastructure’ in Africa, Google Says.” *Reuters*. Accessed December 12, 2024. https://www.reuters.com/technology/fibre-optic-cables-should-be-considered-critical-infrastructure-africa-google-2024-11-14/

Dombrowski, Peter, and Simon Reich. 2024. “Multilateral Maritime Exercises, Grand Strategy, and Strategic Change: The American Case and Beyond.” *Journal of Global Security Studies* 9 (3). https://doi.org/10.1093/jogss/ogae017

Dutch Subsea Cable Coalition. n.d. “Mission Dutch Subsea Cable Coalition.” Accessed November 28, 2024. https://ecp.nl/wp-content/uploads/2023/11/Flyer-Zeekabel-Coalitie.pdf

Dzieza, Josh. 2024. “The Cloud under the Sea.” *The Verge*, April 16, 2024. https://www.theverge.com/c/24070570/internet-cables-undersea-deep-repair-ships

East Micronesia Cable System. n.d. “The Project.” *East Micronesia Cable System*. Accessed December 2, 2024. https://www.eastmicronesiacable.com/the-project

Eighth National People’s Congress. 1997. *Criminal Law of the People’s Republic of China*. http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/13/content_1384075.htm

Elsner, Ivonne, Andreas Huck, and Manas Marathe. 2018. “Resilience.” In *Key Concepts for Critical Infrastructure Research*, edited by Jens Ivo Engels, 31–38. Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-22920-7_4

EU Directorate-General for Maritime Affairs and Fisheries. 2014. “Maritime Security Strategy.” *European Union*, 2014. https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en

euNetworks. 2023. “For the First Time, Researchers Successfully Demonstrate over euNetworks’ Fibre Infrastructure that Quantum Communication Is Possible between the United Kingdom and Ireland,” October 3, 2023. https://eunetworks.com/news/for-the-first-time-researchers-successfully-demonstrate-over-eunetworks-fibre-infrastructure-that-quantum-communication-is-possible-between-the-united-kingdom-and-ireland

eurofiber. 2024. “The IOEMA Project: A new state-of-the-art Data Backbone will provide vital connectivity in the southern North Sea”. 31 May, 2024. https://www.eurofiber.com/press/the-ioema-project-a-new-state-of-the-art-data-backbone-will-provide-vital-connectivity-in-the-southern-north-sea/

European Commission. 2021. “Global Gateway.” *European Commission*, 2021. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en

———. 2022. “Factsheet: Medusa Is by Far the Largest Submarine Cable Project in the Mediterranean to Date with 7,100 km.” November 24, 2022. https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-11/2022-11-24%20-%20Factsheet%20for%20Media%20-%20Medusa.pdf

———. 2023. “EU-NATO Task Force: Final Assessment Report on Strengthening Our Resilience and Protection of Critical Infrastructure,” June 29, 2023, Press Release edition. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564

———. 2024a. “Recommendation on the Security and Resilience of Submarine Cable Infrastructures.” Commission Recommendation C(2024) 1181 final. Brussels. https://digital-strategy.ec.europa.eu/en/library/recommendation-security-and-resilience-submarine-cable-infrastructures

———. 2024b. “Support for the Implementation of Recommendation (EU) 2024/779 on Secure and Resilient Submarine Cable Infrastructures.” EC-CNECT/2024/OP/0070. Brussels. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/de671bd2-aac2-46e4-8824-67a06991179d-CN

———. 2024c. “White Paper - How to Master Europe’s Digital Infrastructure Needs?” COM(2024) 81 final. Brussels. https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

———. 2024d. “The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World”, September 26, 2024. https://digital-strategy.ec.europa.eu/en/library/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world

———. 2025. “EU Action Plan on Cable Security” Brussels, 21.2.2025, JOIN(2025) 9 final. https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables

———. n.d. “PISCES Cable System.” *EU Funding & Tenders Portal*. Accessed December 13, 2024. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/43251567/101133769/CEF2027

European Council. 2020. “How the IPCR crisis response mechanism works”. https://www.consilium.europa.eu/en/infographics/ipcr-mechanism/

———.2023. “Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan”. 24 October 2023. https://www.consilium.europa.eu/media/67499/st14280-en23.pdf#https://www.consilium.europa.eu/media/67499/st14280-en23.pdf

———. 2024. “Critical Infrastructure: Blueprint for protecting EU citizens and the internal market”. 25 June, 2024, https://www.consilium.europa.eu/media/2xfm2tj3/st10653en24.pdf

European Health and Digital Executive Agency. 2024. “CEF-Digital Calls Are Now Open: €323 Million Is Available for Co-Funding the Deployment of Digital Connectivity Infrastructures,” October 22, 2024. https://hadea.ec.europa.eu/news/cef-digital-calls-are-now-open-eu323-million-available-co-funding-deployment-digital-connectivity-2024-10-22_en

Federal Foreign Office Germany. 2024. “Joint Statement by the Foreign Ministers of Finland and Germany on the Severed Undersea Cable in the Baltic Sea.” *Federal Foreign Office Germany*, November 18, 2024. https://www.auswaertiges-amt.de/en/newsroom/news/2685132-2685132

Federal Maritime and Hydrographic Agency of Germany (*Bundesamt für Seeschifffahrt und Hydrographie*).n/d. “Unterwasserkabel (Underwater cables). https://www.bsh.de/DE/THEMEN/Offshore/Offshore-Vorhaben/Unterwasserkabel/unterwasserkabel_node.html

Federal Ministry for Digital and Transport (*Bundesministerium für Digitales und Verkehr*). 2024. "*BMDV veranstaltet Konferenz über Ausbau und Resilienz von Unterseedatenkabeln*" (BMDV Hosts Conference on the Expansion and Resilience of Submarine Data Cables). 02 July 2024. https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2024/056-konferenz-unterseedatenkabel.html

Fígoli, Andrés. 2024. "Legal & Regulatory Matters Year in Review", Fíjoli Consulting, November 24, 2024. https://www.subcables.com/post/submarine-cable-regulations-2024

Fontaine, Jean-Marie. 2018. "Liability for Damage to Underwater Cable under Canadian Maritime Law." *Submarine Telecoms Forum Magazine* 99 (March 2018): 32–37. https://issuu.com/subtelforum/docs/stf-issue_99/32

Franken, Jonas, Thomas Reinhold, Lilian Reichert, and Christian Reuter. 2022. "The Digital Divide in State Vulnerability to Submarine Communications Cable Failure." *International Journal of Critical Infrastructure Protection* 38 (September). https://doi.org/10.1016/j.ijcip.2022.100522

Franken, Jonas, Franziska Schneider, Christian Reuter. 2023. "The Internet's Plumbing Consists of Garden Hoses: A Critical Analysis of the Advantages and Pitfalls of Metaphors Use for Critical Maritime Infrastructures" *Dreizack* 23. Kiel. https://peasec.de/paper/2023/2023_FrankenSchneiderReuter_MetaphernMarKRITIS_Dreizack23.pdf

Franken, Jonas, and Christian Reuter. 2024a. "Secure Critical Infrastructures." In *Information Technology for Peace and Security*, edited by Christian Reuter, 279–301. Technology, Peace and Security I Technologie, Frieden Und Sicherheit. Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-44810-3_13

———. 2024b. "The Subsea Data Cable Security Map – Fusing Public Information for Enhanced Critical Maritime Infrastructure Security" In *Proceedings of the MARESEC 2024*. Bremerhaven: Zenodo. https://doi.org/10.5281/zenodo.14216270

Franken, Jonas, Thomas Reinhold, Timon Dörnfeld and Christian Reuter. 2025. "Hidden Structures of a Global Infrastructure: Expansion Factors of the Subsea Data Cable Network." *Technological Forecasting & Social Change 215* (June). https://doi.org/10.1016/j.techfore.2025.124068

General Assembly. 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." A/70/174. United Nations. https://digitallibrary.un.org/record/799853

———. 2016. "Report of the Open-Ended Intergovernmental Expert Working Group on Indicators and Terminology Relating to Disaster Risk Reduction." A/71/644. United Nations. https://digitallibrary.un.org/record/852089

———. 2023. "Oceans and the Law of the Sea." A/RES/78/69. United Nations. https://digitallibrary.un.org/record/4031021

Green, Mick, and Keith Brooks. n.d. "The Threat of Damage to Submarine Cables by the Anchors of Ships Underway." *Centre for International Law, Lee Kuan Yew School of Public Policy, National University of Singapore*, 1–9. https://cil.nus.edu.sg/wp-content/uploads/2011/04/Mick-Green-and-Keith-Brooks-The-Threat-of-Damage-to-Submarine-Cables-by-the-Anchors-of-Cables-Underway.pdf

Gritten, David, "Crucial Red Sea data cables cut, telecoms firm says", *BBC*, 5 March, 2024. https://www.bbc.co.uk/news/world-middle-east-68478828

Hollick, Matthias, and Stefan Katzenbeisser. 2024. "Resilient Critical Infrastructures." In *Information Technology for Peace and Security*, edited by Christian Reuter, 303–12. Technology, Peace and Security I Technologie, Frieden Und Sicherheit. Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-44810-3_14

Hruska, Joel. 2008. "Undersea Saboteurs May Have Been Responsible for Cable Cuts." *Ars Technica*, February 19, 2008. https://arstechnica.com/uncategorized/2008/02/undersea-saboteurs-may-have-been-responsible-for-cable-cuts

Infocomm Media Development Authority. 2016. "Guidelines on Deployment of Submarine Cables into Singapore."

Infocomm Media Development Authority Statutory Board Under the Singapore Ministry of Digital Development and Information. https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/codes-of-practice-and-guidelines/subcablelanding.pdf

Infocomm Media Development Authority. 2023. "Singapore's Digital Connectivity Blueprint", Ministry of Communications and Information and Infocomm Media Development Authority. https://www.imda.gov.sg/-/media/imda/files/programme/digital-connectivity-blueprint/digital-connectivity-blueprint-report.pdf

———. 2019. "Guidelines on the Management of Submarine Cable Damage Incidents in Singapore Port Limits and the Traffic Separation Scheme Zone." Infocomm Media Development Authority Statutory Board Under the Singapore Ministry of Digital Development and Information. https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/codes-of-practice-and-guidelines/2019-04-01-guidelines-on-the-management-of-submarine-cable-incidents.pdf

International Advisory Body on Submarine Cable Resilience Declaration, February 2025. https://www.itu.int/digital-resilience/submarine-cables/wp-content/uploads/sites/2/2025/02/summit-declaration-nigeria-2025.pdf

International Cable Protection Committee. 2025. "Charting Submarine Cables Is Critical for Maritime Safety & Infrastructure Protection". 27 February 2025, https://www.iscpc.org/publications/icpc-viewpoints/charting-submarine-cables-is-critical-for-maritime-safety-and-infrastructure-protection/

International Cable Protection Committee. 2021. "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables: Best Practices Version 1.2." International Cable Protection Committee. https://www.iscpc.org/publications/icpc-best-practices

———. 2024. "Glossary & Abbreviations." November 25, 2024. https://www.iscpc.org/information/glossary-and-abbreviations

International Law Association. 2024. "Submarine Cables and Pipelines under International Law." Third Interim Report 2024. International Law Association. https://www.ila-hq.org/en/documents/ilathi-1

International Telecommunication Union. 2012. "ITU/WMO/UNESCO IOC Joint Task Force: Joint Task Force to investigate the use of submarine telecommunications cables for ocean and climate monitoring and disaster warning". https://www.itu.int/en/ITU-T/climatechange/task-force-sc/Pages/default.aspx

International Telecommunication Union. 2024. "Launch of International Advisory Body to Support Resilience of Submarine Telecom Cables: Strengthening Resilience of Submarine Cable Networks Is Key to Digital Connectivity and Economies." *International Telecommunication Union*, November 29, 2024. https://www.itu.int/en/mediacentre/Pages/PR-2024-11-29-advisory-body-submarine-cable-resilience.aspx

———. n.d. "Submarine Cable Resilience." *International Telecommunication Union*. Accessed December 16, 2024. https://www.itu.int/en/digital-resilience/submarine-cables/Pages/default.aspx

International Tsunami Information Center. n.d. "1929 Grand Banks Earthquake & Tsunami." *UNESCO/IOC*. Accessed December 12, 2024. https://legacy.itic.ioc-unesco.org/legacy.itic.ioc-unesco.org/index2ad0.html?option=com_content&view=article&id=1458&Itemid=2873

Internet Society. 2024. "2024 West Africa Submarine Cable Outage Report." https://www.internetsociety.org/wp-content/uploads/2024/04/2024-West-Africa-Submarine-Cable-Outage-Report.pdf

Kavanagh, Camino. 2022. "Cyber Incident Classification: A Report on Emerging Practices within the OSCE Region." Vienna: Organization for Security and Co-operation in Europe. https://www.osce.org/files/f/documents/6/5/530293_1.pdf

———. 2023. "Wading Murky Waters: Subsea Communications Cables And Responsible State Behaviour." UNIDIR. https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Wading_Murky_Waters_Subsea_Communications_Cables_Responsible_State_Behaviour.pdf

Kavanagh, Camino, Jonas Franken, and Joanna Kulesza. Forthcoming 2025. “In Oceans and in Orbits: The Infrastructure Essential to the Public Core of the Internet.”

Kazama, Motoki, and Toshihiro Noda. 2012. “Damage Statistics (Summary of the 2011 off the Pacific Coast of Tohoku Earthquake Damage).” *Soils and Foundations* 52 (5): 780–92. https://doi.org/10.1016/j.sandf.2012.11.003

Kington, Tom. 2022. “Italian Navy, telecom provider team up to deter attacks on undersea cables”. July 14, 2024. https://www.defensenews.com/naval/2022/07/14/italian-navy-telecom-provider-team-up-to-deter-attacks-on-undersea-cables/

KIS-ORCA. n.d. “About: The KIS-ORCA Project.” Accessed December 20, 2024. https://kis-orca.org/about

La Junta Directiva de la Autoridad Maritima de Panama. 2024. *Resolución J.D. No. 021-2024*. https://www.gacetaoficial.gob.pa/pdfTemp/30037/104884.pdf

Lartigue, Aurore. 2024. “Câbles sous-marins: en rachetant son fleuron ASN, la France répare une «erreur stratégique” (Submarine cables: by buying back its flagship ASN, France is correcting a ‘strategic mistake), *Radio France Internationale*, November 10, 2024. https://www.rfi.fr/fr/économie/20241110-câbles-sous-marins-en-rachetant-son-fleuron-asn-la-france-répare-une-erreur-stratégique

Legislative Council Panel on Information Technology and Broadcasting Hong Kong. 2007. *Disruption of External Telecommunications Services Due to Earthquakes near Taiwan on 26 and 27 December 2006*. https://www.legco.gov.hk/yr06-07/english/panels/itb/papers/itb0115cb1-697-1-e.pdf

Marle, Graham. 2007. “Subsea Landslide Is Likely Cause of SE Asian Communications Failure.” ICPC Press Release. ICPC Secretariat. https://iscpc.org/documents/?id=9

Marter, Hans J. 2023. “Governments Knew What Caused October Communication Outage but Never Told the Public.” *Shetland News*, January 19, 2023. https://www.shetnews.co.uk/2023/01/19/governments-knew-what-caused-october-communication-outage-but-never-told-the-public/

McBride, Oliver. 2022. “UK-registered fishing vessel damaged Shetland subsea cable”. December 08, 2022. https://thefishingdaily.com/latest-news/uk-registered-fishing-vessels-damaged-shetland-subsea-cable/

McCabe, Robert, and Brendan Flynn. 2024. “Under the Radar: Ireland, Maritime Security Capacity, and the Governance of Subsea Infrastructure.” *European Security* 33 (2): 324–44. https://doi.org/10.1080/09662839.2023.2248001

McLaughlin, Rob, Tamsin Phillipa Paige, and Douglas Guilfoyle. 2022. “Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization.” *Journal of Conflict and Security Law* 27 (3): 297–338. https://doi.org/10.1093/jcsl/krac014

Mentges, Andrea, Lukas Halekotte, Moritz Schneider, Tobias Demmer, and Daniel Lichte. 2023. “A Resilience Glossary Shaped by Context: Reviewing Resilience-Related Terms for Critical Infrastructures.” *International Journal of Disaster Risk Reduction* 96 (103893): 1–28. https://doi.org/10.1016/j.ijdrr.2023.103893

Ministry of Communications, India. 2023. “TRAI releases recommendations on ‘Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India”, 20 June 2023. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1933678

Ministry of Digital Affairs, Denmark. 2024. *The Role of Big Tech as Digital Infrastructure*. November 2024. Copenhagen: Ministry of Digital Affairs. https://www.english.digmin.dk/Media/638736628110392217/The%20role%20of%20big%20tech%20as%20digital%20infrastructure.pdf

Multilateral Cooperation Center for Development Finance. n.d. “Antarctic Submarine Cable.” https://www.themcdf.org/en/what-we-do/projects/2023/Antarctic-Submarine-Cable.html

Murph, Darren. 2008. “Fourth Undersea Cable Cut near UAE, Suspicions Rise.” *Engadget*, February 5, 2008. https://www.engadget.com/2008-02-05-fourth-undersea-cable-cut-near-uae-suspicions-rise.html

National Communications Authority Ghana. 2024. “Undersea Cable Disruptions Affect Data Services,” March 14, 2024. https://nca.org.gh/2024/03/14/undersea-cable-disruptions-affect-data-services

National Science Foundation. 2022. “Exploring the Feasibility of a Science Monitoring And Reliable Telecommunications (SMART) Fiber Optic Cable System Connecting Antarctica Australia New Zealand.” National Science Foundation. https://www.nsf.gov/geo/opp/documents/NSF_Public%20Release%20DTS_Final.pdf

NATO. 2025. “NATO Launches ‘Baltic Sentry’ to Increase Critical Infrastructure Security,” January 14, 2025. https://www.nato.int/cps/en/natohq/news_232122.htm

National People’s Congress (NPC) of the People’s Republic of China, n/d. “Database of Laws and Regulations,” http://www.npc.gov.cn/zgrdw/englishnpc/Law/Frameset-page7.html

New York Times, ‘Undersea Surgeons’, November 29, 2024, https://www.nytimes.com/interactive/2024/11/30/world/africa/subsea-cables.html

Niinistö, Sauli. 2024. “Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness.” European Commission. https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

Noor, Elina. 2024. “Entangled: Southeast Asia and the Geopolitics of Undersea Cables.” *University of Hawaii at Manoa, Center for Indo-Pacific Affairs*, Indo-Pacific Outlook, 1 (5): 1–10. https://manoa.hawaii.edu/indopacificaffairs/article/entangled-southeast-asia-and-the-geopolitics-of-undersea-cables

Oktivana, Davina, and Irkham Afnan Trisandi Hasibuan. 2024. “Indonesia: The Regulation and Protection of Submarine Cables in Indonesia.” ASEAN Academic Reports on Submarine Cables. CIL Academic Symposium. https://cil.nus.edu.sg/wp-content/uploads/2024/05/Combined-ASEAN-Academic-Reports-on-Cables_4-Jun-24-final.pdf

Palmer-Felgate, ‘Global Cable Repair Data Analysis, Edge Network Services Limited., ICPC Annual Plenary, Singapore, 2024.

Palmer-Felgate, Andy, Nigel Irvine, Simon Ratcliffe, and Seng Sui Bah. 2013. “Marine Maintenance in the Zones – A Global Comparison of Repair Commencement Times.” Reading: SubOptic. https://minz.org.nz/i/2018-challenges/Marine-maintenance-in-the-zones.pdf

Parliament of the Cook Islands. 2024. *Manatua Cable Protection Act*. https://parliamentci.wpenginepowered.com/wp-content/uploads/2024/05/Manatua-Cable-Protection-Act-2024.pdf

Petit, Zelie. 2024. “Beneath NATO’s Radars: Unaddressed Threats to Subsea Cables.” *Center for Strategic and International Studies*, December 2, 2024. https://www.csis.org/blogs/strategic-technologies-blog/beneath-natos-radars-unaddressed-threats-subsea-cables

Prime Minister of Australia. 2023. “United States-Australia Joint Leaders’ Statement - Building an Innovation Alliance.”, October 25, 2023. https://www.pm.gov.au/media/united-states-australia-joint-leaders-statement-building-innovation-alliance

Pursiainen, Christer, and Eero Kytömaa. 2023. “From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean?” *Sustainable and Resilient Infrastructure* 8 (sup1): 85–101. https://doi.org/10.1080/23789689.2022.2128562

Qui, Winston. 2024. “Chile Receives 4 Bids on the Feasibilitiy [sic] Study for Antarctica Cable.” *Submarine Cable Networks*, December 12, 2024. https://www.submarinenetworks.com/en/systems/antarctic/chile-antarctic-cable/chile-receives-4-bids-on-the-feasibilitiy-study-for-antarctic-cable

République Française. 2004. *Code Des Postes et Des Communications Électroniques. Section 2; Dispositions Pénales. (Article L73)*. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006465626/2024-12-14

———. 2019. Code Des Postes et Des Communications Électroniques. Section 2; Dispositions Pénales. (Article L81). https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038889134/2024-12-14

Ruffino, Jane. 2024. “Baltic Subsea Cables: A Story of Resilience, Not Fear.” *Internet Society Pulse*, November 22, 2024. https://pulse.internetsociety.org/blog/baltic-subsea-cables-a-story-of-resilience-than-fear

Runde, Daniel F., Erin L. Murphy, and Thomas Bryja. 2024. “Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition.” *Center for Strategic and International Studies*, August 16, 2024. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Ryan, Sophie. 2024. “Submarine Communication Cables and Belligerent Rights in Armed Conflict.” *Ocean Yearbook Online* 38: 459–503.

Scottish Government. 2023. “Correspondence Regarding Shetland Telecommunications Cable Damage: FOI Release.” *Scottish Government*, December 6, 2023. https://www.gov.scot/publications/foi-202200331574

SEA-SPINE. n.d. “SEA-SPINE: High-Speed Submarine Backbone for Islands of the Aegean Sea.” https://sea-spine.eu

Sechrist, Michael. 2012. “New Threats, Old Technology Vulnerabilities in Undersea Communications Cable Network Management Systems.” Discussion Paper #2012-03. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/sechrist-dp-2012-03-march-5-2012-final.pdf

Secrétariat général de la mer. 2020. “Circulaire: Attractivité Du Territoire Français En Matière de Câbles Sous-Marins de Communication.” Réf : 142 /SGMer. Paris: Secrétariat général de la mer. https://www.info.gouv.fr/upload/media/organization/0001/01/sites_default_files_contenu_piece-jointe_2021_03_142-20201113-sgmer-attractivite_en_matiere_de_cables_sous_marins.pdf

Sherman, Justin. 2021. “Trend 2: Companies Using Remote Management Systems for Cable Networks.” *Atlantic Council*, September 1, 2021. https://www.jstor.org/stable/resrep35117.7

SMART Cables. 2024. “SMART Systems.” *SMART Cables*, 2024. https://www.smartcables.org

Solon, Olivia and Hatem, Mohammed, “Damaged Subsea Cables Repaired in Red Sea”, *Bloomberg*, July 17, 2024. https://gcaptain.com/damaged-subsea-cables-repaired-in-red-sea/

Speidel, Ulrich. 2022. “The Hunga Tonga Hunga Ha’apai Eruption – A Postmortem: What Happened to Tonga’s Internet in January 2022, and What Lessons Are There to Be Learned?” In *Proceedings of the 17th Asian Internet Engineering Conference*, 70–78. Hiroshima: ACM. https://doi.org/10.1145/3570748.3570759

Starosielski, Nicole et al. 2025, “Report on Strategic Network Resilience in the Caribbean. SubOptic Foundation (forthcoming 2025).

State Council of the People’s Republic of China. 1989. *Provisions Governing the Laying of Submarine Cables and Pipelines*. https://faolex.fao.org/docs/pdf/chn150001E.pdf

Submarine Cable Infrastructure Expert Group. 2024. “Follow-up on Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures.” E03940. Register of Commission Expert Groups and Other Similar Entities (European Commission). https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3940&newsTypeId=1

SubTel Forum. 2022. *Industry Report*. Vol. 11. Industry Report. Submarine Telecoms Forum. https://issuu.com/subtelforum/docs/submarine_telecoms_indsutry_report_issue_11

Sun, Zhen. 2018. “Protection of Cable Ships Engaged in Operations for Submarine Telecommunication Cables.” *Ocean Development & International Law* 49 (2): 118–33. doi:10.1080/00908320.2018.1452386

Supreme Court of Canada. 2014. “Peracomo Inc. v. TELUS Communications Co.” Supreme Court Judgements 34991. https://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/13612/index.do

Tammikko, Teemo. 2024. “The EU and NATO in Pursuit of Better Deterrence: Baltic Sea Sabotage Prompts Rethink of Current Practices”. Finnish Institute of International Affairs. February 2024. https://fiia.fi/wp-content/uploads/2025/02/BP404_The-EU-and-NATO-in-pursuit-of-better-deterrence.pdf

TeleGeography. 2024. “Submarine Cable Map.” *TeleGeography*, 2024. https://www.submarinecablemap.com

The Crown Estate. 2023. “The Crown Estate to Digitally Map Scenarios to Inform Co-ordinated Approach to Future Seabed Use”. June 13, 2023. https://www.thecrownestate.co.uk/news/the-crown-estate-to-digitally-map-scenarios-to-inform-co-ordinated-approach

The Communications Security, Reliability and Interoperability Council IV. (2014). “Working Group 8 Final Report 1: Spatial Separation”. December, 2014. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG8_Report1_3Dec2014.pdf

The European Parliament, and The Council. 2021. *Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240 (Text with EEA Relevance)*. https://eur-lex.europa.eu/eli/reg/2021/694/oj

———. 2022a. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. https://eur-lex.europa.eu/eli/dir/2022/2555

———. 2022b. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC*. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

———. 2022c. *Proposal for a Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

———. 2022d. *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

———. 2023. “Summary of Directive (EU) 2018/1972 European Electronic Communications Code,” April 11, 2023. https://eur-lex.europa.eu/EN/legal-content/summary/european-electronic-communications-code.html

The Nanfang Daily. 2024. “广东海警侦破一起特大海缆损坏案 [Guangdong Marine Police Detected a Large Sea Cable Damage Case],” January 15, 2024. http://www.gd.gov.cn/gdywdt/zfjg/content/post_4331799.html

The Parliament of the Commonwealth Australia, House of Representatives. 2005. *Telecommunications and Other Legislation Amendment (Protection of Submarine Cables and Other Measures) Bill 2005 Explanatory Memorandum*. https://www8.austlii.edu.au/au/legis/cth/bill_em/taolaoscaomb2005936.pdf

UK Department for Science, Innovation & Technology. 2024. “DSIT Areas of Research Interest 2024.” *Department for Science, Innovation & Technology*, February 26, 2024. https://www.gov.uk/government/publications/department-for-science-innovation-and-technology-areas-of-research-interest/dsit-areas-of-research-interest-2024

UK Maritime & Coastguard Agency. 2021. “MGN 661 (M+F) Navigation - Safe and Responsible Anchoring and Fishing Practices.” *Guidance Gov.uk*, December 1, 2021. https://www.gov.uk/government/publications/mgn-661-mf-navigation-safe-and-responsible-anchoring-and-fishing-practices/mgn-661-mf-navigation-safe-and-responsible-anchoring-and-fishing-practices

UK Ministry of Defence, UK Foreign, Commonwealth and Development Office, The Rt Hon Sir Keir Starmer KCB KC MP, and The Rt Hon John Healey MP. 2025. "Joint Expeditionary Force Activates UK-Led Reaction System to Track Threats to Undersea Infrastructure and Monitor Russian Shadow Fleet," January 6, 2025. https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet

UK National Archives. n.d. "United Kingdom Hydrographic Office (UKHO) Archive Cables Records.", https://archive.ukho.gov.uk/records/CAB

UltramapGlobal. 2024. "The Biggest Threat to Subsea Cables." *UltramapGlobal*, August 4, 2024. https://ultramapglobal.com/the-biggest-threat-to-subsea-cables

Union of the Comoros. 2024. *Décret N°24-003PR portant promulgation de la loi N°23-024AU portant modification de la loi N°14-031/AU du 17 mars 2014 relative aux Communications Electroniques* https://munganyo.km/decrees/168

United Kingdom. 1885. *Submarine Telegraph Act 1885*. https://www.legislation.gov.uk/ukpga/Vict/48-49/49

United Nations Office of Counter-Terrorism, and Counter-Terrorism Committee Executive Directorate. 2018. "The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices." United Nations. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

United States. 1888. *Submarine Cable Act 1888*. https://govtrackus.s3.amazonaws.com/legislink/pdf/stat/25/STATUTE-25-Pg41a.pdf

US Department of State. 2024a. "National Security Memorandum on Critical Infrastructure Security and Resilience." *US Department of State*, May 3, 2024. https://irp.fas.org/offdocs/nsm/nsm-22.pdf

———. 2024b. "United States International Cyberspace & Digital Policy Strategy: Towards an Innovative, Secure, and Rights-Respecting Digital Future." US Department of State. https://www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

US Federal Communications Commission. 2024. "Review of Submarine Cable Landing License Rules and Procedures to Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks; Amendment of the Schedule of Application Fees Set Forth in Sections 1.1102 through 1.1109 of the Commission's Rules." Notice of Proposed Rulemaking FCC-CIRC2411-01. Washington, DC: Federal Communications Commission. https://docs.fcc.gov/public/attachments/DOC-407142A1.pdf

US Code (2021). United States Code, 2021 Edition. Title 46 – Shipping, Subtitle V – Merchant Marine, Part C, Chapter 532 – Cable Security Fleet. https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title46-chapter532&edition=prelim

US Department of Homeland Security. 2024. "Priorities for DHS Engagement on Subsea Cable Security & Resilience: A White Paper by the Office of Economic Security, DHS Supply Chain Resilience Center, and US Cybersecurity and Infrastructure Security Agency." https://www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf

US Office of the Federal Register. 2024. *Code of Federal Regulations: Title 47 § 4.15 Submarine Cable Outage Reporting*. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-4/subject-group-ECFRb4cb67a8301113e/section-4.15

Valentia Transatlantic Cable Foundation. 2024. "Valentia Island Subsea Cable Security and Resilience Symposium." Valentia Island Transatlantic Cable Station, Valentia Island, Co. Kerry, Ireland: Valentia Transatlantic Cable Foundation. https://symposium.valentiacable.com

Veverka, Dean. n.d. "Under the Sea." Shipping and Marine. Accessed January 22, 2025. https://www.iscpc.org/documents/?id=201

Waagaard, Ole Henrik, Jan Petter Morten, Erlend Rønnekleiv, and Steinar Bjørnstad. 2022. “Experience from Long-Term Monitoring of Subsea Cables Using Distributed Acoustic Sensing.” In *27th International Conference on Optical Fiber Sensors*, Th2.4. Alexandria, Virginia: Optica Publishing Group. https://doi.org/10.1364/OFS.2022.Th2.4

Wall, Colin, and Pierre Morcos. 2021. “Invisible and Vital: Undersea Cables and Transatlantic Security.” *Center for Strategic and International Studies*, June 11, 2021. https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Wilson, George Grafton. 1901. *Submarine Telegraphic Cables in Their International Relations: Lectures Delivered at the Naval War College*, August, 1901. US Government Printing Office. https://archive.org/details/submarinetelegr01sgoog

Wishart, Beatrice. 2022. “Question Reference: S6W-12519.” *The Scottish Parliament*, November 24, 2022. https://www.parliament.scot/chamber-and-committees/questions-and-answers/question?ref=S6W-12519

Yee, William Yuen. 2023. “Laying Down the Law Under the Sea: Analyzing the US and Chinese Submarine Cable Governance Regimes.” *The Jamestown Foundation China Brief*, 4 August, 2023. https://jamestown.org/program/laying-down-the-law-under-the-sea-analyzing-the-us-and-chinese-submarine-cable-governance-regimes

Zain, Asma Ali. 2008. “Cable Damage Hits One Million Internet Users in UAE.” *Khaleej Times Online*, February 4, 2008. https://web.archive.org/web/20080209140523/http://www.khaleejtimes.com/DisplayArticleNew.asp?section=theuae&xfile=data%2Ftheuae%2F2008%2Ffebruary%2Ftheuae_february121.xml

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais des Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG