IN-DEPTH ANALYSIS

Requested by the SEDE sub-committee

European Parliament

Security threats to undersea communications cables and infrastructure – consequences for the EU

Authors:

Christian BUEGER, Tobias LIEBETRAU, Jonas FRANKEN

European Parliament coordinator:

Policy Department for External Relations

Directorate General for External Policies of the Union

PE 702.557 - June 2022

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

IN-DEPTH ANALYSIS

Security threats to undersea communications cables and infrastructure – consequences for the EU

ABSTRACT

The EU's subsea data cable network is both vital for global connectivity and vulnerable. This study provides a systematic review of the current security threats, as well as the actors at the origin of these threats. Building on reports and expert input, the paper takes stock of current awareness, preparedness and response mechanisms, both at the EU and Member State level. A number of recommendations suggest how to improve the resilience of the cable network. Proposals build on the need to enhance EU-wide awareness, improve coordination and share information across EU institutions and Member States. In addition, surveillance capabilities must be advanced, response and repair mechanisms strengthened, and the topic mainstreamed across external action.

EP/EXPO/SEDE/FWC/2019-01/LOT4/1/C/12
April 2022 - PE 702.557

EN

AUTHORS AND CONTRIBUTORS

Authors

- Christian BUEGER, Professor of International Relations, Department of Political Science, University of Copenhagen, Denmark & Honorary Professor, University of Seychelles, Seychelles;
- Tobias LIEBETRAU, Postdoctoral Researcher, Centre de Recherches Internationales (CERI), Sciences Po Paris, France;
- Jonas FRANKEN, Research Assistant, Science and Technology for Peace and Security (PEASEC), Technical University of Darmstadt, Germany.

Research Assistance

- Anna SARASIBAR, Junior Consultant Security & Justice, Ecorys, The Netherlands;
- Jan ESSINK, Junior Consultant Security & Justice, Ecorys, The Netherlands;
- Tyren KONING, Student Assistant Security & Justice, Ecorys, The Netherlands.

The chapters 2 and 3 draw on research funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE and by the LOEWE initiative (Hesse, Germany) within the emergenCITY centre. Dipl.-Inf. Thomas REINHOLD (Technical University Darmstadt) provided valuable advice and support for both chapters.

PEER REVIEWER

- Lars GJESVIK, Research Fellow at NUPI's Centre for Digitalization and Cyber Security Studies from the Norwegian Institute for International Affairs, Oslo, Norway.

PROJECT COORDINATOR (CONTRACTOR)

- Alexandra RIMPLER-SCHMID, Senior Consultant Security & Justice, Ecorys, The Netherlands.

This paper was requested by the European Parliament's sub-committee on Security and Defence (SEDE).

CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Jérôme LEGRAND, Policy Department for External Relations

Editorial assistant: Grégory DEFOSSEZ

Feedback is welcome. Please write to jerome.legrand@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu

VERSION

English-language manuscript completed in April 2022.

COPYRIGHT

This paper will be published on the European Parliament's online database, 'Think Tank'

Table of contents

List of abbreviations

ACGF	Arctic Coast Guard Forum
ACMA	Atlantic Cable Maintenance & Repair Agreement
AIS	Automated Identification System
ANSSI	L'Agence Nationale de la Sécurité des Systèmes
CIPD	(Maltese) Critical Infrastructure Protection Directorate
CISE	(EU's) Common Information Sharing Environment
CMR	(EU's) Critical Maritime Routes (Programme)
CSDP	(EU's) Common Security and Defense Policy
DGSE	(French) Direction Générale de la Sécurité Extérieure
DKCPC	Danish Cable Protection Committee
DSR	(China's) Digital Silk Road
ECGFF	European Coast Guard Functions Forum
EDA	European Defense Agency
EEA	European Environmental Agency
EEAS	European External Action Service
EFCA	European Fishery Control Agency
EMA	(French) État-Major des Armées
EMASOH	European Maritime Awareness Strait of Hormuz (operation)
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cyber Security
EP	European Parliament
EUMC	EU Military Committee
EUMSS	European Union Maritime Security Strategy
EUROSUR	European Border Surveillance System
Frontex	European Border and Coast Guard Agency
HARMSPRO	(EU's) Harbour & Maritime Surveillance and Protection
HRVP	High Representative of the European Union for Foreign Affairs and Security Policy
ISAC	(EU's) Information Sharing and Analysis Centre
IcSP	(EU's) Instrument contributing to Stability and Peace
ICD	Improvised Cutting Devices
INTCEN	(EU) Intelligence and Situation Centre
ISPS	International Ship and Port Facility Security (Code)
IXP	Internet Exchange Point

MARSUR	(EU's) Maritime Surveillance project
MAS	(Danish) Marine Assistance Center
MAS MCM	(EU's) Maritime (semi-) Autonomous Systems for Mine Countermeasures
MCA	Malta Communication Authority
MEAE	(French) Ministère de L'Europe et des Affaires Étrangeres
MIC-RAN	Maritime Intelligence Agency & Risk Analysis Network
MIED	Maritime Improvised Explosive Devices
MECMA	Mediterranean Cable Maintenance Agreement
MENA	Middle East and North Africa
MEP	Member of European Parliament
MROSS	(UK's) Multi-Role Ocean Surveillance Ship
MUSAS	(EU's) Maritime Unmanned Anti-Submarine System
NACGF	North-Atlantic Coast Guard Forum
NDICI	(EU's) Neighbourhood, Development and International Cooperation Instrument
PESCO	(EU's) Permanent Structured Cooperation Committee
SEDE	(European Parliament's) subcommittee on Security and Defence
SGM	(French) Secretariat Général à la Mer
UNCLOS	United Nations Convention on the Law of the Sea
UNODC	UN Office on Drugs and Crime

Executive summary

The global subsea data cable network is a vital critical infrastructure. As much as 99 % of the world's digital communications transit through the network, and the global economy and digital services are fully dependent on it. Since cables lay out at sea, across national borders and are often hidden underground, they have frequently been forgotten and received limited attention from policymakers. Sparked by Russian naval activity since 2014 and the geopolitical shockwaves sent by the 2022 Ukraine war, the vulnerability of maritime infrastructures is now receiving growing public and policy attention. Yet, as this report shows, European governance of cable protection and resilience still lags behind and needs improvement. The EU and its Member States will have to address the vulnerabilities of European digital connectivity. The report proposes several measures that the EU could implement and provides recommendations to the European Parliament on how it can steer this development.

Chapters 1 and 2 detail the scope and methodology of the report and discuss how important the cable network is in global connectivity, the digital economy, and military operations.

Chapters 3 and 4 provide an in-depth analysis of the EU's dependencies on the cable network and the vulnerabilities that the EU faces. They also offer an introduction to the key legal and technical features of the network. We conclude that the EU has growing redundancy, which means that the impact of minor damages can be managed well, yet a number of very vulnerable sites exist.

Chapter 5 analyses the threats to the EU from Russia, China and other states, as well as from extremist groups and transnational crime networks. It shows that several states have both the capabilities and the intent to potentially cause harm to EU connectivity. While we evaluate the risk of a major breakdown as low, considering it could equate to an act of war, symbolic attacks on cable connections are to be expected. Attacks and sabotage by extremists and criminal groups are equally probable.

Chapter 6 reviews the awareness and measures available to EU Member States. We show that cable protection is an issue of growing concern in public debates and in national security strategies in countries such as France, Portugal and Ireland. In other states, government awareness is rather limited. States have advanced different models of how they govern cables. In states such as France and Portugal, cable security is a key issue for naval forces. Others, such as Malta, rely on governance systems under civilian leadership. Yet, in others, such as Denmark, the governance of cables is led by the industry. The fact that cables often cross different mandates, responsibilities and jurisdictions poses a significant trans-European governance challenge. This calls for an intra-EU dialogue on best practices governing and protecting cables at a state level.

Chapter 7 surveys the awareness and programmes at the EU level. Cables protection is an issue in maritime security, cyber security, ocean governance and infrastructure policies. This implies that several Directorates and technical agencies have a role in ensuring cable protection and resilience (including EMSA, EFCA, Frontex, and ENISA). While cables and other maritime infrastructures are frequently mentioned in EU strategies, hardly any actions and programmes address the issue directly. A similar picture arises in relation to external action, where EEAS and EDA run relevant programmes, which, however, only address the issue tangentially. Cable resilience is also a key issue in EU-NATO relations and for future relations with the UK.

Chapter 8 provides a range of recommendations for taking steps towards better cable resilience that need urgent attention. Our recommendations include:

First, awareness of the issue must be increased. The update of the EU Maritime Security Strategy (EMSA) and the review of the mandate of EMSA provide key opportunities here. But the lack of awareness also calls for other dedicated measures.

Secondly, information sharing on cable governance, incidents, and suspicious activity needs to be improved. We recommend installing a cable resilience coordination group in the Commission that would include cable industry representatives.

Thirdly, additional measures are needed to strengthen the surveillance of cables at the EU level. Partially, the technology is already in place, yet, EMSA does not have the respective mandate, and cable surveillance does not feature in CISE yet. Technological advancements in subsea surveillance that could be steered through EDA on subsea surveillance systems are also an important option.

Fourthly, since cable connections are transnational and key in developing global digital connectivity and the economy, external action must take the issue more seriously. Dedicated 'cable diplomacy' and capacity building programmes are needed.

In summary, we recommend that the European Parliament steers the debate by increasing awareness and inviting the Commission and the HRVP to develop initiatives and actions for coordination, surveillance and external action.

1 Introduction

1.1 Objectives and scope

The objective of this study is threefold. First, it provides Members of the European Parliament (MEPs) and interested members of the public with the first systematic analysis of the vulnerability of European states to cable failures due to deliberate attacks. This includes an evaluation of the state and non-state actors from which such threats might stem. Second, the study shows which scenarios stand to affect EU Member States. We then discuss the current awareness and programmes in a selected number of EU Member States and at the level of European institutions and policy processes. The last objective of the study is to provide recommendations to improve the resilience of EU's undersea cable infrastructure. These are formulated on the basis of conclusions drawn from the analysis. In terms of scope, threats from within and outside of the EU are considered. The EU's dependencies and existing and potential forms of collaboration with partners are addressed on a global scale.

1.2 Methodological approach

The study was conducted by Ecorys and three experts between December 2021 and April 2022. Information was collected through extensive desk research and review of key strategies, policy documents, incident reports and studies published on the issue, and thematic interviews and written inputs from practitioners and advisers from a range of backgrounds. These include the Danish Subsea Cable Protection Committee, the European Fishery Control Agency, the European Maritime Safety Agency, the European Subsea Cable Association, the European Union Agency for Cybersecurity, and cybersecurity and maritime security experts.[1]

The security of subsea cable infrastructure is a problem that has hardly been studied and systematically analysed, and only a handful of policy reports or legal studies exist. In this sense, the results of this study are ground-breaking and novel on the one hand, but limited in scope on the other. We focus on open data, a selected number of cases and rely on expert interviews. This implies that a detailed investigation of how different European states regulate and protect their cables still remains to be done. Much of the data concerning the military dimension of data cable resilience is not in the public domain or is heavily classified. This implies that an in-depth analysis of the ways that defence capabilities depend on the subsea data cable network remains a task to be done. Given the ongoing focus on integrated, digitally mediated and autonomous defence capabilities, such dependencies are most likely substantial.

1.3 Structure of the study

The report first outlines the context and relevance of the study in Chapter 2, followed by an overview of the EU's cable infrastructure in Chapter 3. Chapter 4 analyses the EU's vulnerability and causes of harm to cable infrastructure. Chapter 5 provides a comprehensive threat analysis, and Chapter 6 provides an overview of member state awareness. Chapter 7 provides a review of awareness and responses on EU level. Chapter 8 delivers recommendations on reinforcing EU preparedness.

[1] See annex II for a list of consulted organisations

2 Context and relevance of the study

2.1 Importance of digital economy and digital sovereignty

The Submarine data cable network is the core critical infrastructure of the digital age. The network is composed of fibre optic cables laid on the ocean floor and digitally connects countries worldwide.[2] These cables, which are often thousands of kilometres in length, transmit high volumes of data rapidly from one point to another. As much as 99 % of the world's digital communications transit through the global cable network. Undersea cables are the backbone of the global economy, with roughly USD 10 trillion in financial transactions transmitted via these cables each day.

There are more than 400 active cables worldwide, spanning at least 1.3 million kilometres.[3] This makes the undersea data cable network a physical manifestation of transnational digital connectivity. Undersea cables are critical for intra-European communication and connecting European states to the world.

Beyond use for civilian purposes, countries depend on undersea cables for national security. The coordination of military operations, diplomatic missions and the collection of intelligence depend on the cable network. The loss of communications for a few minutes or hours can have disastrous repercussions in time-sensitive operations and can have high financial implications. The implications of any form of cable damage are therefore significant.

[4]

2.2 Unintentional human activity

The most common damage caused to undersea cables is human error and negligence (see chapter 3). 40 % of cable disruptions arise from bottom-tending commercial fishing equipment and related dredging. Another 15 % of damage is caused by anchoring incidents, such as improperly stored anchors, anchoring outside approved areas, sea conditions affecting anchor positioning, and the emergency dropping of an anchor. Other benign human factors include dredging and dumping, oil and gas development, offshore wind and energy development, hydrokinetic projects, ocean thermal energy conversion, and deep-sea mining operations.

[2] D. Swinhoe, 'What is a submarine cable? Subsea fiber explained', *Data Center Dynamics*, 26 August 2021.
[3] TeleGeography, 'Submarine Cable Frequently Asked Questions', n.d.
[4] Shutterstock commercial picture database.

2.3 Intentional human activity

The potential for sabotaging undersea cables during times of conflict, as part of grey zone or hybrid warfare operations or by transnational terrorism and organised crime exists, but such incidents have not been confirmed yet.

The security and resilience of undersea cables is an understudied element of international security.[5] Given that internet access and data are defining resources of the twenty-first century, protecting submarine cables is far too essential a domain of international politics to remain a technical addendum to security analysis. It concerns how our digital futures will be governed and how a global free, open, and secure circulation of data can be ensured. Due to the crucial role of undersea cables and the growing concerns around their security, it is paramount for the European Union and its Member States to ensure the protection of submarine cables.

2.4 Significance of cables infrastructure

While wireless and satellite technologies are continuously developed and deployed, submarine cables remain the fastest, most efficient and least expensive way to send digital information across the globe for the foreseeable future. With the current trend toward remote work, the increasing use of cloud storage and the arrival of 5G and the Internet of Things, industrial production, public services, and the lives of everyday citizens will become even more dependent on the smooth working of undersea cables.

2.5 The paradox of invisibility of cable infrastructure

Submarine data cables have only very recently seen increasing political and scholarly attention. Over the past five years, concerns over their protection have increasingly emerged in public debates. In particular military leadership has expressed public worries about the vulnerabilities of the cable network (see chapter 6). While there is a growing awareness, there continues to be a lack of care among policymakers and regulators. Part of the reason is the invisibility of this infrastructure. Physically, submarine cables lie underground, and they are out at sea, rendering them largely invisible. There is a tendency to pay little attention to what happens at sea more generally —a phenomenon that has been described as collective sea blindness.[6] Like other types of infrastructure, they often go unnoticed until they fail.[7] When streets close, shipping routes are blocked, or the electric power grid fails, we recognise our dependency on them.

Yet, paradoxically, the invisibility of cables is also what protects them. While roughly marked on maps to avoid accidental damage by users of the sea, their invisibility implies that it is more difficult to target them in deliberate attacks.

2.6 The complexity of governing cable infrastructure

The undersea cable network is part of a very complex set-up of diverse actors operating, regulating and protecting the infrastructure. Their regulation and protection cut through conventional separation of labour in many ways. While telecommunication agencies are often the lead actors in protection at a national level, their security depends on maritime law enforcement and surveillance in coastal zones (e. g., coast guards, marine police, and when situated in marine protected areas, even marine rangers). Further out at sea, undersea cables depend on military protection. At a policy level, the cable infrastructure straddles different policy fields, including maritime security, cyber security, digital, infrastructure,

[5] As reviewed in C. Bueger, and T. Liebetrau, 'Governing hidden infrastructure: The security politics of the global submarine data cable network', *Contemporary Security Policy*, *42*(3), pp. 391-413.
[6] C. Bueger, and T. Edmunds, 'Beyond Seablindness: A New Agenda For Maritime Security Studies, International Affairs', *International Affairs*, *93*(6), pp. 1293–1311.
[7] C. Bueger, and T. Liebetrau, 'Governing hidden infrastructure: The security politics of the global submarine data cable network', *Contemporary Security Policy*, *42*(3), pp. 391-413.

telecommunications, fishery, shipping, and marine environment protection. This is also reflected at the EU level, where a broad range of agencies, including the European Maritime Safety Agency, the European Fishery Control Agency, the European Union Agency for Cybersecurity, and several Directorates of the European Commission, e.g. DG Connect, DG MOVE, or DG MARE, have mandates which are related and relevant. No agencies, however, are focused or leading on the issue.

The planning, production, operation, and maintenance of undersea cables are almost entirely in the hands of the private sector. Some of the largest suppliers include Alcatel Submarine Networks and Nexans (France), Prysmian Group (Italy), NKT A/S (Denmark), SubCom (United States), NEC (Japan), and Huawei Marine Networks (China). The market share of Chinese run companies has significantly increased over the years. Network operators have traditionally been the main investors in undersea cables. Still, Big Tech companies (e.g., Google, Amazon, Microsoft, Facebook) are expanding their investments in this sector to ensure the interconnection of their data centres. While often interpreted falsely as a niche market, submarine data cables are a major vector of influence for companies on the global internet, including its functioning, development and security.

2.7 Transnational dimension

Cable systems establish particular forms of transnational relations that often extend or transcend conventional bilateral or regional forms of cooperation. Some countries, such as the United Kingdom, France, or Egypt, have a particularly important position in the international cable system, acting as connecting points between political regions.

The applicable international legal regime is sometimes perceived as outdated and unfit for the challenges of today.[8] As shown in chapter 5, legal responsibilities differ between territorial water and non-territorial waters[9]. The United Nations Convention on the Law of the Sea (UNCLOS) prescribes that coastal states have the right (but not the obligation) to adopt regulations to protect submarine cables in their territorial waters.[10] Concerning the areas outside of the territorial waters of the coastal states, UNCLOS does not provide an obligation to specific states to safeguard submarine cables but instead allocates an obligation to all states to adopt regulations that ensure that ships under their flag are punished for destroying or damaging a submarine cable.[11]

[8] K. Scott, 'Laws governing undersea cables have hardly changed since 1884 – Tonga is a reminder they need modernizing', *The Conversation*, 21 January 2022; R. Beckman, 'Submarine Cables – A Critically Important but Neglected Area of the Law of the Sea', *ISIL Conference*, 2010, pp. 12-16.
[9] T. Davenport, 'Submarine Cables, Cybersecurity: an Intersectional Analysis', *Catholic University Journal of Law and Technology*, *24*(1), 2015, pp. 57-109.
[10] United Nations Convention on the Law of the Sea, Article 21(c), 1982.
[11] United Nations Convention on the Law of the Sea, Article 113, 1982.

3 The connectivity of Europe. An overview of cable infrastructure and how it matters

The internet is the central medium of present times, connecting more than 4.66 billion people worldwide.[12] Within the EU, 92 % of households are equipped with internet access.[13] Despite the internet's apparent far-reaching distribution and growing importance for individuals as well as societies, its basic enabling physical infrastructures remain largely unknown and unseen to the majority of users. Cell towers and household Wi-Fi routers are the only physical internet providing infrastructures visible in everyday life. The internet backbone is a complex network of highly capable fibre-optic data cables that connect continents, countries, and islands. These cables are hidden mainly underground or on the seafloor. They bundle the data traffic of the more than 27 billion individual end devices.[14] While doing so, they transmit around 140 Terabytes of data per second[15] at nearly the speed of light on several wavelengths simultaneously. Submarine cables carry approximately 99 % of international internet traffic.[16] Thus, they handle most of the data sent and distances bridged.

3.1 The EU's dependence on digital connectivity

Online data traffic is nearly impossible without functioning submarine cables. In the past, cable failures triggered internet blackouts, i.e., sustained and widespread total collapse of internet connectivity.[17] In global comparison, all EU members have reached a high level of digitalization, internet penetration, and internet usage.[18] These indicators point out the growing dependencies on the internet in multiple areas, internally and externally. Below some key aspects are described to highlight the internal and external dependency of the EU on a functioning submarine cable infrastructure:

Economy: Most transactions and communication in economic life in the internal market of the EU are handled online. 94 % of EU's businesses have a fixed broadband connection, and 78 % have a website. 41 % of all European enterprises use tools like cloud services that require a permanent internet connection, and for large enterprises, this share grows to 71 %.[19] Since many server infrastructures of cloud providers are located outside the EU, international data traffic is required to use these services. Recently, the Covid-19 pandemic accelerated the shift from traditional offline business services to contemporary internet-based processes. Without the internet, most businesses would not be able to uphold their work routines, connect with customers, authorities, and companies, or even generate profit.

Like the internal market, the EU depends on a functioning global trade system for its external economy. These systems are hardly imaginable without a stable internet connection, giving access to databases, orders, customers, and suppliers.

Critical infrastructures: According to the proposed EU Directive on the resilience of critical entities (CER Directive), '*"Critical infrastructure" means an asset, facility, equipment, network, system or part thereof, which*

[12] International Telecommunication Union (ITU), 'Measuring digital development: Facts and Figures 2021', 2021.
[13] Eurostat, 'Statistics Explained: Digital economy and society statistics – Household and individuals', *European Commission*, 2021.
[14] Cisco, 'Cisco Annual Internet Report (2018–2023)', 2020.
[15] Internet Live Stats, 'One Second', 2021.
[16] J. Baumann, 'Publisher of subsea cable news uses ArcGIS for industry analysis and interactive mapping', *Submarine Telecoms Magazine*, 2021, p. 36–37 ; NATO Cooperative Cyber Defence Centre of Excellence, 'Strategic importance of, and dependence on, undersea cables', 2019; D. Winseck, 'The Geopolitical Economy of the Global Internet Infrastructure', *Journal of Information Policy*, 2017, p. 228–267.
[17] P. Menon and Tom Westbrook, 'Undersea cable fault could cut off Tonga from rest of the world for weeks', reuters.com, 18 January 2021.
[18] International Telecommunication Union (ITU), 'World Telecommunication/ICT Indicators Database online 23rd Edition', 2019.
[19] Eurostat, 'Statistics Explained: Digital economy and society statistics – Enterprises: Access and use of the internet', *European Commission*, 2021.

is necessary for the provision of a […] service […] indispensable for the maintenance of vital societal functions or economic activities.'[20] Various critical infrastructures are increasingly dependent on a stable internet connection. Examples of these services can be found in the finance sector (internet-based ATMs), transport sector (coordination systems for to-the-minute supply chains), water and food sectors (digitalised water supply systems and smart agriculture). The finance system, especially high-frequency trading, is dependent on a functioning fibre-optic link between the global marketplaces. No other means of communication can transmit the required mass of information at this speed over long distances. Cloud-stored health data and eGovernment approaches further intensify the internet dependency on essential public services.

Security and Defence: With the move to digital communications in policing and the digital systems of cross-border traffic, the internal security of the EU and its Member States is highly dependent on digital connectivity. In the age of digital warfare and integrated platforms, the majority of the EU Member States' defence capabilities are connected digitally. This relates to command-and-control structures but also integrated weapon systems, including drones and aircraft carriers.

Society: Current social life depends on internet connections more than ever before. Social media and online messengers offer quick and effective ways to communicate and organise. Large parts of crisis communication and disaster warning presently rely on internet technologies, making them irreplaceable in these scenarios.

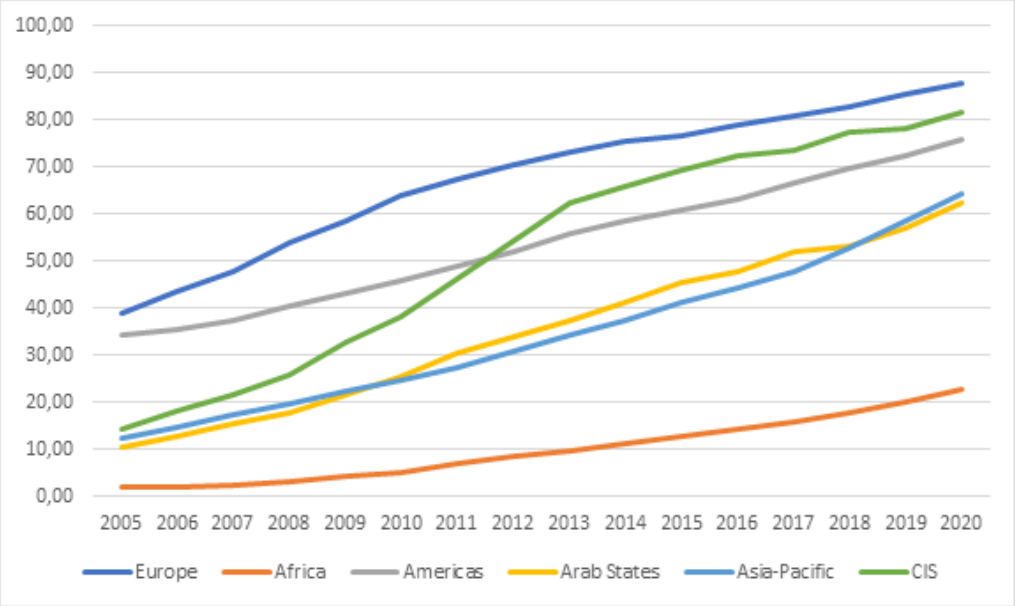

Figure 1: Percentage of households with internet access in six world regions (Source: own representation, based on ITU Statistics) [21]

3.2 The EU's cable infrastructure

About 250 cable systems connect the EU to the global internet. Two-thirds are submarine cables laid in the surrounding seas, namely the Atlantic, Mediterranean, North Sea, and Baltic Sea. One-third of international cables are land-based cables that connect EU Member States with non-EU-members sharing a land

[20] European Commission, 'Proposal for a Directive of the European Parliament and the of the Council on the resilience of critical entities', 14262/20 + ADD1, 2020/0365 (COD), 2021.
[21] International Telecommunication Union (ITU), 'Measuring digital development: Facts and Figures 2021', 2021.

border.[22] While the following primarily focuses on undersea cables, the important role of land-based cables in the internet backbone should not be overlooked. Some EU Member States situated in continental Europe predominantly rely on these for trans-border connections, while others achieve a high level of redundancy through the combination of land and sea, as explained in Figure 2. In general, island states and overseas territories are more vulnerable to submarine cable failure because they lack the potential to gain access to land-based fibre-optic networks.[23]

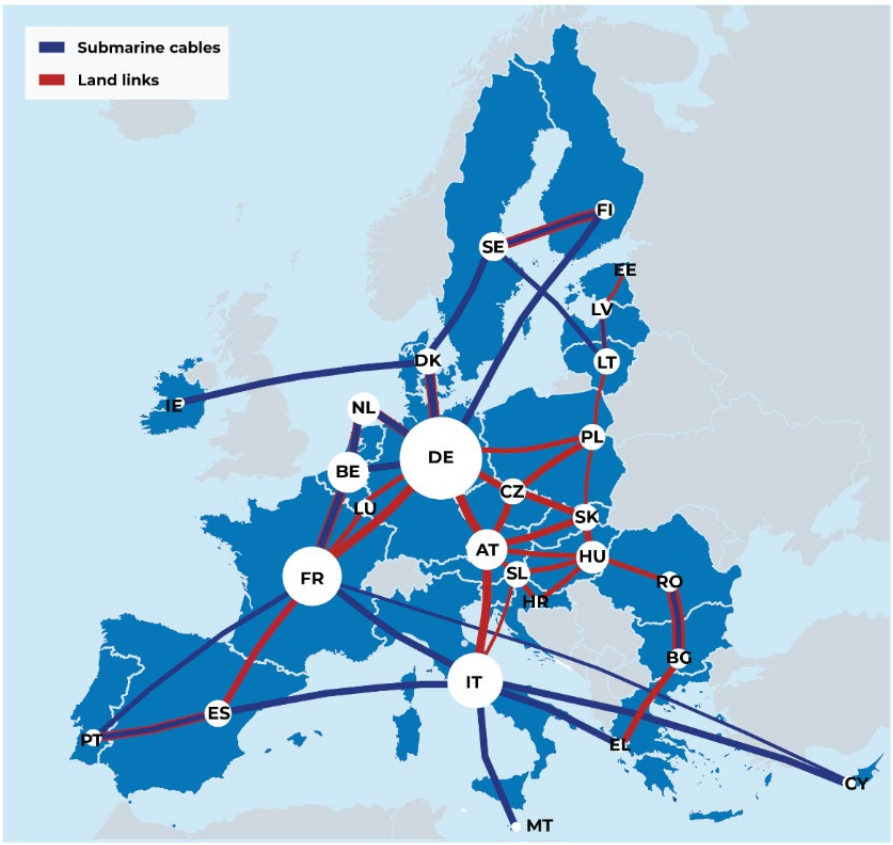

Figure 2: Internal connections between the EU27 Member States over submarine cables (blue) and terrestrial links (red) (Source: own representation).

The density of submarine cable connections between different world regions varies enormously. First, looking at the internal links **within the EU**, there is a dense network of 39 active submarine cables (see Figure 4).[24] These are necessary to cross the Baltic, the Mediterranean and the North Sea in order to include Sweden, Finland, and the island Member States (Ireland, Malta, Cyprus) in the European backbone network. For coastal member states characterized by peninsular shape (Denmark, Spain, Italy, Greece) or large shares of coastline (Portugal, France, Estonia, The Netherlands), the submarine cables offer an economical and convenient way to enhance access to the internet.

Comparing the **external connectivity of the EU to other world regions**, the transatlantic connections to **North America** are strongest in terms of their cumulative transmission capacity.[25] With the end of the

[22] International Telecommunication Union (ITU), 'Interactive Transmission Map', 2020.
[23] International Telecommunication Union (ITU), 'Small Island Developing States (SIDS) and ICTs', 2019.
[24] Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[25] Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.

United Kingdom's EU membership, the number of EU's direct transatlantic links was reduced from 18 to 11.[26] However, Brexit does not have a direct impact on the current data traffic because the internet's fundamental routing principle is oblivious to national political borders. Even in a scenario of inactive UK cables, there is no threat to the transatlantic connectivity of the EU.[27] The most recent, highly capable transatlantic cable projects such as MAREA, Dunant, or Havfrue circumvent the UK, with landings in France, Spain, and Denmark.[28]

The connections from the EU to **Eastern and Southern Asia**, through the Mediterranean, the Suez Canal, the Red Sea, and the Indian Ocean are strong amounting to about ten cable systems that connect both regions.[29]

Some of these systems branch out to countries in the **Middle East and North Africa** (MENA) region, making the connection of the EU to the MENA countries quite diverse. The cross-Mediterranean networks between Southern Europe and the Maghreb subregions are particularly close-meshed. Overall, 27 active cable connections between the EU Member States and the MENA region are installed.[30]

A lower level of links exists between the EU and **Western, Eastern, and Southern African** countries. Only three cable systems directly connected to the EU supply the vast coastline, but newly planned cable systems (Equiano, 2 Africa, PEACE, Africa 1) will alleviate that situation by 2023.[31] With the ongoing installation of a denser network of land-based fibre-optic cables in many African countries, installing cable systems that circle the whole continent may become less necessary.

For **South and Central America**, European internet traffic was usually passing through North Atlantic cables to the US. With the recent EllaLink project and the older systems of Atlantis 2 and COLUMBUS III, there are only three direct links between the European Union and Latin America.[32] The EU's connections to the polar region (Iceland and Greenland) and Russia have a similarly low connection density. Also, there are no direct links between the EU and **Australia/Oceania** and the **Antarctic**. Figure 3 gives an overview of the interregional submarine cable connections.

[26] Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[27] R. Miller, 'Brexit Prep Has Boosted Data Centers, Subsea Cables', Data Center Frontiers, 2019.
[28] Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.
[29] Infrapedia, 'Infrastructure Map', 2021; TeleGeography, 'Submarine Cable Map', 2021.
[30] Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.
[31] Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.
[32] International Telecommunication Union (ITU), 'Interactive Transmission Map', 2020; Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.

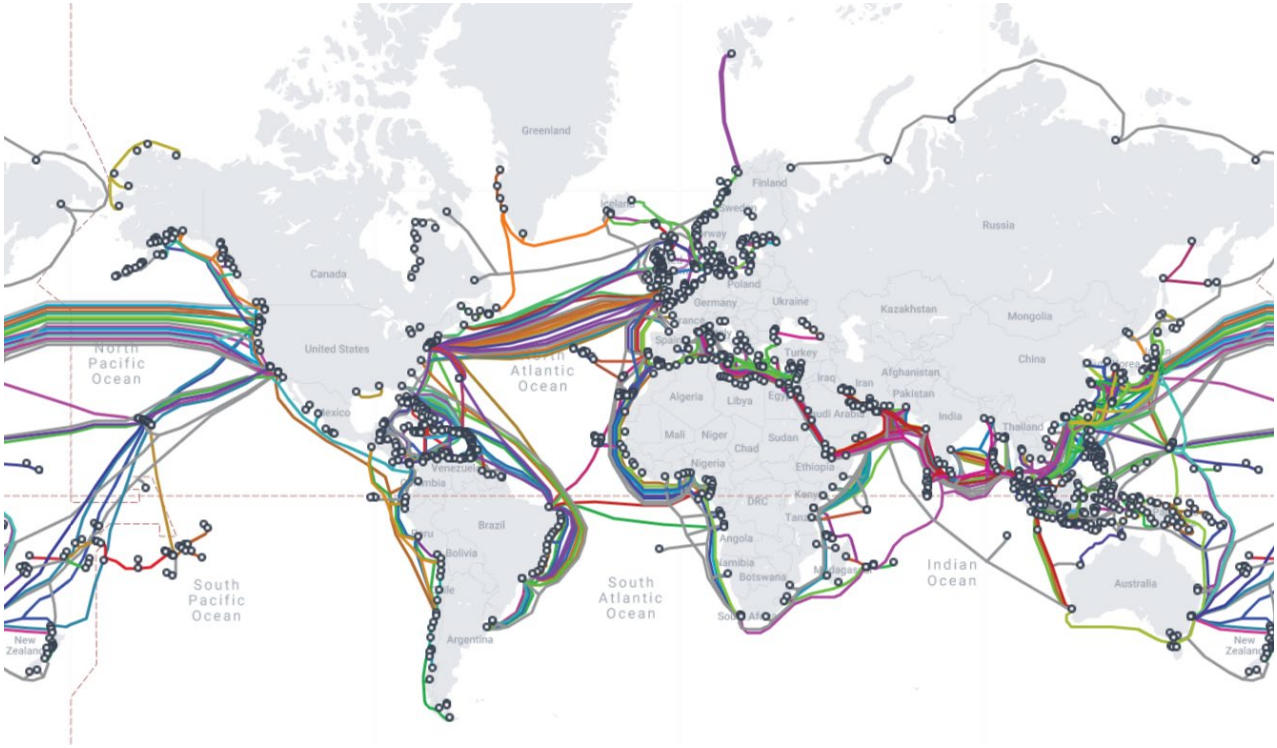

Figure 3: Submarine cable connections between world regions. In terms of the numbers of cables, Europe and MENA have the strongest connection (27 cable systems) and Australia/Oceania and the MENA the weakest (one cable system). (Source: TeleGeography[33])

3.3 The key landing sites

The location of cable landing stations is vital to the resiliency of the cable infrastructure. If multiple cable landings are constructed in mutual proximity, there is an enhanced risk of failure due to the same disruption event, see Section 4.2 below.

For the EU, some locations stand out as favoured landing sites. Marseille is the central hub for data traffic to the MENA region and Asia, with twelve active or planned systems.[34] Before the UK left the EU, most transatlantic traffic entered the EU on the English southwestern coast (Bude, Porthcurno, Highbridge).[35] After Brexit, these cables are still in use, but the data now enters the EU after crossing the English Channel. For the 28 links between the EU and the UK, the cable landing hotspots in Calais (FR), Oostende (BL), and Zandvoort (NL) are the most important.[36]

[33] Teleography, 'Submarine Cable Map', 11 April 2022.
[34] International Telecommunication Union (ITU), 'Interactive Transmission Map', 2020; K. Paximadis, and C. Papapavlou, 'Towards an all New Submarine Optical Network for the Mediterranean Sea: Trends, Design and Economics', *12th International Conference on Network of the Future (NoF)*, 2021; Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[35] International Telecommunication Union (ITU), 'Interactive Transmission Map', 2020; K. Paximadis, and C. Papapavlou, 'Towards an all New Submarine Optical Network for the Mediterranean Sea: Trends, Design and Economics', *12th International Conference on Network of the Future (NoF)*, 2021; Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[36] International Telecommunication Union (ITU), 'Interactive Transmission Map', 2020; K. Paximadis, and C. Papapavlou, 'Towards an all New Submarine Optical Network for the Mediterranean Sea: Trends, Design and Economics', *12th International Conference on Network of the Future (NoF)*, 2021; Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.

Reconsidering the submarine cable network resiliency, recently planned cable projects diversify the location of cable landing stations.[37] Increasingly, new cable landings of high-capacity projects at the French and Danish West coasts, as well as Bilbao, indicate a change of mindset in the landing location planning. Implementing geographical distances between cable landing stations reduces the risks of simultaneous failures. Detaching the locations of cable landing stations from large settlements or port facilities further reduces the risk of damages.

3.4 Data centres and internet exchange points

Besides submarine and land-based cable structures, two other components are vital to the functioning of the internet: Data Centres and Internet Exchange Points (IXPs).

The former serve as storage facilities for computer systems and the massive amounts of necessary data, like webpages and their contents, that can be accessed through the internet. The hotspots of data centre locations within the EU are Frankfurt (54 centres), Amsterdam (41), and Paris (31). Massive clusters of data centres exist in Stockholm (29), Milan (22), Dublin (19), Sofia (20), Madrid (19), Bucharest (19), Copenhagen (17), Riga (17) and Helsinki (17).[38] And most importantly, there is no EU member state without at least seven data centres, enabling storage of data within EU borders. In the future, the number of data centres will continue to grow due to the proliferation of technological innovations in the context of digitalisation, e.g., cloud computing, the Internet of Things, or artificial intelligence applications.

Internet Exchange Points (IXP), in turn, enable the transmission and exchange of data among different Internet Service Providers and local telecommunication companies. There, the providers of local and regional networks are connected to the internet backbone structures of the providers of international and intercontinental networks, enabling their customers to access the global network. In the EU, the Netherlands have the most IXP (106), followed by Germany (83), France (35), and Italy (34).[39] Without these essential data hubs, a countries' network traffic must be routed outside of its territory in order to be forwarded. However, all Member States have at least one facility, and they are generally technologically advanced, making this scenario highly unlikely.

The submarine cables are owned mainly by conglomerates of private telecommunication companies with diverse national headquarter.[40] While the information on cable owners is widely available,[41] there is little information on the operators and buyers of the capacities. Content-providing tech giants like Microsoft, Amazon, Meta, and Google have built and co-financed their own cable systems in recent years.[42] Examples of high-capacity cables of this kind with EU landings are the Dunant (Google: France), Havrue (Meta, Google: Denmark, Ireland), and the MAREA cables (Meta, Microsoft: Spain).

[37] R. Miller, 'Brexit Prep Has Boosted Data Centers, Subsea Cables', Data Center Frontiers, 2019.
[38] Data Center Map ApS, 'Data Center Map', 2022.
[39] Infrapedia, 'Infrastructure Map', 2022.
[40] Infrapedia, 'Infrastructure Map', 2021; Submarine Telecoms Forum, 'Industry Report 2021/2022', 2021.
[41] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.
[42] A. Mauldin, 'A Complete List of Content Providers' Submarine Cable Holdings', TeleGeography, 2021; Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.

4 An analysis of the EU's vulnerability

This section first reviews the different types of causes of harm to the cable network. We then explore key factors of vulnerability and proceed in outlining the most vulnerable Member States and regions.

4.1 Overview of vulnerabilities and causes of harm

Multiple causes potentially render submarine data cables incapable of data transmission. Around 100 cable ruptures happen each year globally.[43] End users hardly notice those faults because the data traffic is usually rerouted through alternative cable paths. Total internet outages only occur when there is no broadband redundancy available. It is helpful to form categories to differentiate between the various fault scenarios.[44] Roughly speaking, there are three causes of faults: natural, human, and external.

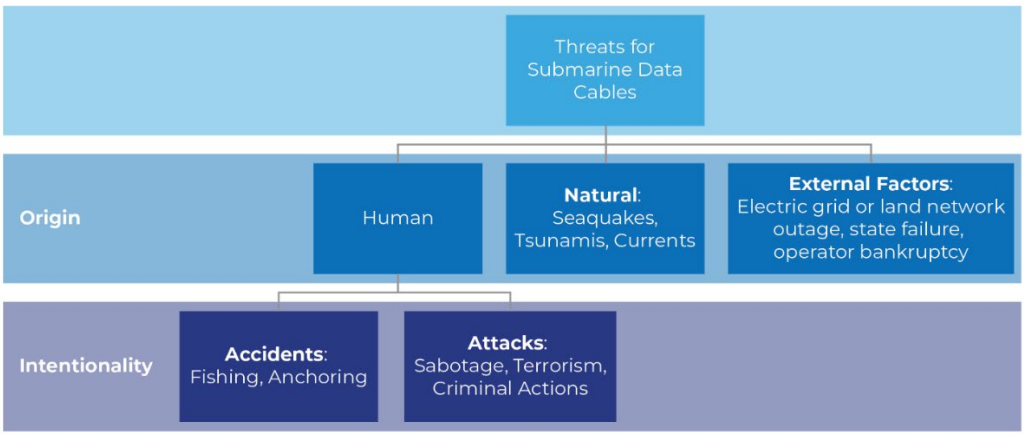

Figure 4: Threat types for submarine data cables (own representation)

4.1.1 Natural causes

First, cable rupture can be the outcome of natural disasters like seaquakes and other seismic activity, tsunamis, and underwater currents during storms. Further natural factors are long-term processes that may lead to abrasion of the protective layers of cables, such as corrosion, tide, and weather-related currents. Natural impacts account for about one-fifth of cable incidents.[45] These kinds of cable damages are less likely than human-caused, accidental cable breaks. However, they bear the potential of multiple simultaneous failures. For example, in the aftermath of the Tōhoku earthquake of 2011, four of 20 submarine cables to Japan ruptured.[46] These simultaneous outages seriously impacted inter-Asian and transpacific internet traffic.[47] In this case, the loss of bandwidth could be compensated with Japan's remaining cables. For territories with fewer redundancies, parallel breaks have a higher probability of complete internet blackout.

[43] D. Swinhoe, 'What is a submarine cable? Subsea fiber explained',*Datacenterdynamics*,26 August 2021.
[44] G. Aceto, A. Botta, P. Marchetta, V. Persico, and A. Pescapé, 'A Comprehensive Survey on Internet Outages', *Journal of Network and Computer Applications*, Issue 113, March 2019, pp, 36–63.
[45] A. Mauldin, 'Cable Breakage: When and How Cables Go Down', *TeleGeography,* 3 May 2017.
[46] W. Qiu, 'Submarine Cables Cut after Magnitude - 9.0 Earthquake and Tsunami in Japan', Submarine Cables Network, 12 March 2011.
[47] E. Strickland, 'Why the Japan earthquake didn't take down the country's internet: The undersea cable network that connects Japan to the world is damaged, but working', *IEEE Spectrum*, March 2011.

4.1.2 Human causes

Human-caused damages to submarine cables are either intentional, caused by negligence, or unintentional. The majority of accidents occur as a consequence of everyday maritime activities, with fishing, anchoring, and dredging most frequently the cause of damage. Of such, mainly unintended cable damages by commercial marine activity amount on average to more than 70 % of the yearly incidents.[48] This large share can be explained by unintended accidents rooted in unfamiliarity with legal rules and protection zones or negligent behaviour and deliberate risk-taking when operating near cable installations. While such accidents are the key source of damage to the cable infrastructure, intentional damages are conceivable scenarios discussed in Chapter 5.

4.1.3 External factors

The final category of submarine cable dysfunctions is related to the external infrastructures and necessary services they depend on. First, fibre-optic data cables longer than 150 km require electric power to function because repeaters need to compensate for signal losses over distance.[49] As a rule, the electricity can be supplied from each landing station of a cable, making a data cable power outage scenario less probable. However, extensive power outages that affect both cable landing stations result in loss of connectivity. Second, the loss of land-based regional communication infrastructures (cables, data centres, IXP), whether for physical (destruction) or non-physical (censorship, routing failures) reasons, renders international submarine cables useless.[50] Another factor that is often overlooked is the roles of cable operators. If security for the cable operating enterprises and their personnel cannot be provided, lack of maintenance threatens the function of a submarine cable in the long term. The same consequence is probable for cases of bankruptcy of cable operating enterprises.

4.2 Key vulnerability factors

With an average ocean depth of 3682m[51], the 1.3 million km[52] of submarine cable infrastructure is installed in a challenging environment. This context makes underwater visual monitoring for most cable sections impossible and even pushes remote-controlled technical gear to its limits. The deep sea thereby offers protection from sabotage while making repairs in cases of cable ruptures complex missions. The average repair of an undersea cable amounts to more than two weeks.[53] Multiple variables factor into the vulnerability of a cable connection[54].

4.2.1 Maritime traffic and infrastructures

Cables located in or close to areas of dense maritime activity from shipping, fishing or leisure crafts and other offshore infrastructures (pipelines, wind parks) are threatened by equipment (fishing nets, anchors) and construction works (dredging).

4.2.2 Geological factors

Seismic activity in the oceans leads to earthquakes, seaquakes, and volcanic eruptions that, in turn, result in underwater landslides and tsunamis. The massive forces that affect cables in these situations have the

[48] A. Mauldin, 'Cable Breakage: When and How Cables Go Down', *TeleGeography*, 3 May 2017.
[49] G. P. Agrawal, 'Optical Communication: Its History and Recent Progress', *In Optics in Our Time*, 2016, pp. 177–199.
[50] A. R. Gohdes, 'Pulling the plug', *Journal of Peace Research*, *52*(3), 2015, pp. 352–367; G. Aceto, A. Botta, P. Marchetta, V. Persico, and A. Pescapé, 'A Comprehensive Survey on Internet Outages', Journal of Network and Computer Applications, Issue 113, March 2019, pp, 36–63.
[51] National Oceanic and Atmospheric Administration Ocean Exploration, 'How deep is the ocean?', 2021.
[52] Submarine Telecoms Forum, 'Industry Report 2021/2022', 2021.
[53] A. Palmer-Felgate, and P. Booi, 'How resilient is the global submarine cable network?', *SubOptic*, 2016, pp. 1–7.
[54] Y. Yincan, J. Xinmin, P. Guofu, and J. Wei (Eds.), 'Safety of Submarine Optical Cable', *Submarine Optical Cable Engineering*, 2018, pp. 235–257.

potential to cause breakage. In territories surrounded by active seismic areas, such as some Greek islands or Cyprus, cable routes and landing stations are particularly vulnerable and require dedicated route planning.

4.2.3 Service lifetime

The longer a cable is subject to tide and surface weather-related currents, the higher the probability of failure through abrasion. However, this kind of failure rarely occurs, and, in many cases, the cables survive their projected service life of 25 years on average without any material failure.

4.2.4 Areas of competing claims

Even though UNCLOS offers clear rules for jurisdiction and the formation of maritime zones, there are areas of competing claims. The largest part of the submarine cables is located within the high seas, where there is almost no legal protection provided – besides Art. 113-115 of UNCLOS. However, states can exert more regulative privileges concerning submarine cables within their territorial waters and exclusive economic zones. If the jurisdiction over submarine cables is unclear, competitive regulative measures or military actions may threaten their security. The only contested maritime areas of concern in the EU which contain cable systems are the Aegean Sea (Greece versus Turkey) and the Levantine Sea (Greece and Cyprus versus Turkey).[55] Although territorial claims are mainly motivated by oil and gas extraction rights, cable systems like MedNautilus and the BlueMed project cross these contested zones and could be subject to differing perceptions of state jurisdiction between EU members and non-members.

4.2.5 Dual-use aspects

The larger the extent of the military purpose of a submarine cable, the higher its probability is to be targeted in a conflict. For example, submarine cables connecting naval bases and satellite receiving stations are characterised by a larger share of military use, making them reasonable targets. In parallel, the few submarine cables that act as passive-sonar ocean research or surveillance systems may be specifically targeted by countries that are interested in hiding their submarine movements.[56] Unless their destruction offers a definite military advantage, data cables intended for civilian data traffic should be protected as civilian objects under humanitarian law.[57] Even in the latter case, the rule of proportionality should govern the attacks, thereby prohibiting attacks with civilian consequences in excessive relation to the military advantage.[58] In order to uphold that status, cable systems should not be equipped with devices and landing on stations that would clearly make them a legally acceptable target in armed conflicts.

[55] C. Schaller, 'Streit im östlichen Mittelmeer – Griechenland, Türkei, Zypern. Eine seevölkerrechtliche Einordnung', *Deutsches Institut für Internationale Politik und Sicherheit*, 2022.
[56] N. Agarwala, '"Green cables" – Development, opportunities and legal challenges: Part I', *Maritime Affairs: Journal of the National Maritime Foundation of India*, 2018, *14*(2), pp. 49–62; N. Agarwala, 'Green cables – Development, opportunities and legal challenges: Part-II', *Maritime Affairs: Journal of the National Maritime Foundation of India*, *15*(1), 2019, pp. 93–107.
[57] International Committee of the Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts', *32nd International Conference of the Red Cross and Red Crescent, 32IC/15/11*, 2015; International Committee of the Red Cross, 'Customary IHL Database: Rule 8. Definition of Military Objectives', n.d..
[58] Article 51(5)(b), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3.

4.2.6 Maritime bottlenecks

Globally, a few maritime chokepoints[59] stand out because of their high density of cables and maritime traffic. For the EU, the most important ones are:

- The Strait of Gibraltar, between Morocco and the Iberian Peninsula. The Strait, connecting the Mediterranean and the Atlantic, is a densely used space for marine activity, including submarine activities. Seven intercontinental cables are passing through the Strait.[60]
- The most vital bottleneck for the EU concerns the passage between the Indian Ocean and the Mediterranean via the Red Sea because the core connectivity to Asia runs via this route.[61] While maritime traffic transits the Suez Canal, the 16 intercontinental cables use a route on the Egyptian mainland adjacent to the canal to avoid damage.

Thus, for the EU, the relations with Morocco, but in particular with Egypt, are vital to ensure digital connectivity. While a route through Israel and the Gulf of Aqaba provides a theoretical alternative to the Egyptian route, such a pathway would likely be vulnerable, even if it would decrease the dependency on Egypt.

The severity of the consequences of a cable rupture depends on four additional key factors:

- **Redundancy level**

The more alternative land and undersea cables there are to balance out the loss of bandwidth from a broken cable, the higher the probability of uninterrupted data traffic. Island territories characterised by zero or only one redundancy to a submarine cable are hence particularly vulnerable.[62] In the future, low-earth-orbit satellite internet technologies might provide part of the answer to provide emergency redundancy.[63]

- **Repair capacities**

A key factor is the availability of repair capacities. The availability and distance to repair capacities, including cable laying and repair vessels, trained personnel, and material, determine how long a break prevails.[64]

- **Simultaneity of incidents**

Since they are often co-located, several submarine cables can sometimes break simultaneously, most conceivably during large natural disasters or through coordinated acts of sabotage. In these scenarios, repair capacities can become scarce, resulting in longer repair times. Higher availability of redundancies – more submarine cables – and alternative internet-providing options are then required.

[59] Choke points are strategic, narrow passages that connect two larger areas to one another. When it comes to maritime trade, these are typically straits or canals that see high volumes of traffic because of their optimal location, see: 'Mapping the World's Key Maritime Choke Points', C. Ang, Visual Capitalist, 30 March 2021.
[60] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.
[61] V. Coffey, 'Sea change: The challenges facing submarine optical communications', *Optics and Photonics News*, 2014, *25*(3), pp. 26–33.
[62] J. Franken, T. Reinhold, L. Reichert, and C. Reuter, 'The Digital Divide in State Vulnerability to Submarine Communications Cable Failure', *International Journal of Critical Infrastructure Protection (IJCIP),* 2022 (forthcoming).
[63] The ongoing construction of internet providing mega-constellations of satellites, primarily SpaceX's Starlink and Amazon's Project Kuiper, may in near future provide broadband access at almost every location worldwide without being dependent on large submarine or terrestrial installations. Unlike the international fibre-optic cables, the small receiving stations can be run with household power generators, offering independent internet access in emergency and catastrophic scenarios.
[64] A. Palmer-Felgate, N. Irvine, S. Ratcliffe, and S. S. Bah, 'Marine maintenance in the zones: A global comparison of repair commencement times', *Suboptic Conference: From Ocean to Cloud*, 2013, pp. 1–6.

- **Internet usage and blackout preparedness**

States marked by very high rates of internet use and large shares of digitalised processes, such as the EU member states, risk suffering severely from an internet outage. Scenario exercises may help states prepare a strategy for the occurrence of total internet blackouts – potentially resulting from submarine cable breaks.

4.3 Key vulnerabilities of EU Member States

The continental EU Member States are connected by a tight network of terrestrial and submarine connections. All continental EU Member States are linked to at least two other members either by land or sea cable systems. On average, non-island EU Member States have 4.5 internal cross-border cable systems available.[65] During partial failures of components, internet traffic is rerouted so that dysfunctions are circumvented, making state-wide internet blackouts highly improbable for the EU Member States.[66] On average, submarine cables have only used 18 % of their maximum capacity.[67] However, island territories are generally more vulnerable to undersea cable-related internet outages because they lack access to dense land-based cable networks. Therefore, the EU island Member States and overseas territories are covered below:

Although an island state, the **Republic of Ireland** has been situated at an EU external border with Northern Ireland since Brexit. However, the future relations with Northern Ireland are not finalised and remain unclear. At present, there is only one cross-border land-based cable, which has been in service since 1999.[68] This single alternative to undersea data traffic is probably not sufficient to meaningfully compensate for the loss of bandwidth after a failure of the – relatively new and many – submarine cables that connect the Republic of Ireland to the US, the UK, Canada, France, Denmark, Iceland (planned 2022), and Norway (planned 2023).[69] Among those, with regard to the six submarine cables with a design capacity above 1TB/s, this scenario is improbable to occur anyway. The landing station diversity of Ireland is particularly advantageous because the cable routes come from multiple directions, thereby minimising the risks of simultaneous failure.

Malta accesses the internet backbone through five submarine data cables, all with Italian nodes on the other end.[70] This number provides sufficient redundancies, even in most scenarios of multiple failures, making internet outages in Malta highly unlikely in the current situation. However, two minor concerns can be raised about the Maltese position in the network. First, the status of cable landing stations on the northern part of its coastline is problematic. While Malta itself has a comparably low level of seismic risks, the north-eastern Mediterranean is the most active area in Europe. These historically infrequent occasions of tsunamis originating from these areas could strike multiple cables in Malta at once.[71] Second, Gozo, the second-largest island of the Maltese Archipelago with 31 000 inhabitants, is connected by only one submarine cable to the local Maltese network.[72] Here, a cable rupture would result in an internet blackout for the rural island.

[65] Infrapedia, 'Infrastructure Map', 2022; TeleGeography, 'Submarine Cable Map', 2021.
[66] Submarine Telecoms Forum, 'Industry Report 2021/2022', 2021.
[67] Submarine Telecoms Forum, 'Industry Report 2021/2022', 2021.
[68] Infrapedia, 'Infrastructure Map', 2022.
[69] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022.
[70] Infrapedia, 'Infrastructure Map', 2022.
[71] P. Galea, 'Seismic history of the Maltese islands and considerations on seismic risk', *Annals of Geophysics*, *50*(6), 2007, pp. 725-740.
[72] Infrapedia, 'Infrastructure Map', 2022.

Seven active submarine cables provide **Cyprus**' internet backbone access.[73] The island state is connected to Turkey, France, Egypt, Israel, Greece, and the currently longest cable system SEA-ME-WE-3.[74] Similar to both examples above, this cable diversity results in a high level of redundancy availability, rendering an internet blackout after cable ruptures very improbable. Yet, Cyprus is situated in a risky seismic area.[75] Therefore, cable landing stations need to be protected from extreme weather events, and the current diversity of supply directions maintained.

Further, some overseas territories belonging to the EU are islands as well:

Of the **French overseas territories**, the Caribbean islands of Saint Martin, Guadeloupe, and Martinique are reasonably well connected to the neighbouring islands, with at least five submarine cables each.[76] The Indian Ocean islands of Mayotte (three cables) and La Réunion (five cables) achieve an appropriate level of redundancy as well.[77] Since its connection to the EllaLink project, the coastal territory of French Guiana is equipped with good redundancy. Considering the cross-border links to Suriname and Brazil, French Guiana is highly unlikely to suffer an internet outage due to backbone failure.

The **Portuguese** Island of Madeira has seven adjacent cables, providing many alternative data traffic routes during downtimes of cables.[78] On the other hand, the Azores are only connected to two cable systems (CAM Ring and COLUMBUS III), offering only little redundancy in case of a cable break.[79] The risk of simultaneous failure is enhanced because both cables land in the exact location.

The **Spanish** Canary Isles are connected to six submarine cables, providing many options for alternate data flow – to West Africa and Europe.[80] Therefore, the risk level for an internet blackout after cable failure is low.

[73] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum, 'Industry Report 2021/2022', 2021.
[74] F. Pirio, and J.B. Thomine, 'The Sea-Me-We 3 undersea cable system', *Optical Fiber Communication Conference and Exhibit. Technical Digest Conference Edition*, 1998, pp. 273–274.
[75] D. Kazantzidou-Firtinidou, N. Kyriakides, R. Votsis, and C. Z. Chrysostomou, 'Seismic risk assessment as part of the National Risk Assessment for the Republic of Cyprus: from probabilistic to scenario-based approach', Natural Hazards, 2022.
[76] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[77] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[78] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[79] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.
[80] Infrapedia, 'Infrastructure Map', 2022; Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022; TeleGeography, 'Submarine Cable Map', 2021.

5 Threat analysis with a focus on deliberate attacks

In this chapter, we conduct a threat analysis with a focus on deliberate attacks by state and non-state actors. By deliberate attacks, we refer to activities that intentionally target the cable network in order to cause damage for political objectives or private gains. We start by revisiting the key components of the cable network, arguing that these are differently affected. We then summarise the key attack scenarios and evaluate the capabilities and intents of different actors.

5.1 Key vectors and threat scenarios

5.1.1 Components of the infrastructure

In order to get a good understanding of the threats of a deliberate attack, it is useful to investigate the architecture and key components of the infrastructure briefly. This includes firstly the cable, secondly, the landing stations, and thirdly, the repair capacities.

- **Cable infrastructure**

The vulnerability of the cable component differs depending on its position. In coastal and shallow waters, the location of cables is usually publicly available to prevent accidents by anchoring and dredging. Positions are marked on navigational charts to ensure awareness of marine users. By contrast, precise locations are not published in the high sea, and cables are hence much more difficult to locate. Depending on how deep the seafloor is, repairs on the high sea are more difficult and time-consuming. That implies a breakage there has a more severe impact than one in coastal waters.

From a legal viewpoint, it is important to recognise that the legal status of cables substantially differs across the different legal zones established by UNCLOS.[81] Countries have full jurisdiction over the cable in their territorial waters, i.e. up to 12 nautical miles (or about 22 kilometres) from the baseline of their coastline. States also have particular law enforcement duties and obligations in the contiguous zone (24nm). States do not have jurisdiction over cables outside those zones. Indeed, on the high seas (the areas outside of national jurisdiction) as well as the Exclusive Economic Zones of states (200 nm), the legal status of cables and rights and responsibility for their protection is ambiguous.[82]

- **Landing stations**

In landing stations, undersea network traffic terminates and connects to the terrestrial network of the local operator. Landing stations tend to be close to the shore and are often collocated with submarine electricity networks or other critical infrastructures.[83] Landing stations host servers, routing and switching technologies that provide the bridge to the terrestrial network. They tend to be physically protected by fences or barb wire and remote surveillance equipment, such as cameras and sensors. The precise locations of landing stations are not in the public domain, although there are indicative maps that potentially make these easy to identify. Indeed, a transnational landing station 'spotting community' exists that aims to take photographs of landing stations and post their precise location on the internet fora.[84]

[81] For a thorough legal analysis of the cables, see D. R. Burnett, R. Beckman, and T. M. Davenport (Eds.), 'Submarine Cables. The Handbook of Law and Policy', 2013; and D. Shvets, 'The International Legal Regime of Submarine Cables: a Global Public Interest Regime', *PhD thesis*, 2020.
[82] International Relations and Defence Committee, 'UNCLOS: the law of the sea in the 21st century', *United Kingdom House of Lords*, 2022.
[83] O. Courtois, C. Bardelay-Guyot, 'Architectures and management of submarine networks', in J. Chesnoy (Ed.), *Undersea Fiber Communication Systems (Second Edition)*, 2016, pp. 343-380.
[84] For examples in the cable spotting community see for instance: 'Submarine cables – resources on the web **Serious nerd alert**', P. Walter, *Liberal Burblings*, 23 September 2014.

The majority of recent cable systems have built-in surveillance capabilities. Distributed Acoustic Sensing is a 'technology that enables continuous, real-time measurements along the entire length of a fibre optic cable.'[85] This technology utilizes the entire optical fibre as the sensing element. These systems allow acoustic signals to be detected over large distances and in harsh environments. They can be used to detect movements and vibrations in the vicinity of the cable, for instance, from shipping activities. These systems are the key instrument for the operating industry to determine when and where breakage or damage has occurred. They are hence vital to ensure fast repair processes, and data from these systems are also used in court proceedings on damages and compensation.

- **Repair capacities**

Cable repair and maintenance is handled by an industry that is separate from the operating and owning companies. Operators and owners enter into 'contracts with marine maintenance companies that have cable and equipment storage depots and cable ships strategically positioned throughout the world, available on a 24/7 standby basis to repair cable faults.'[86] Cable maintenance is organised via global zones and non-profit cooperative agreements, of which two are directly relevant to Europe. The Atlantic Cable Maintenance & Repair Agreement, known as ACMA, covers the Atlantic, focusing on the North Sea and the Southern Europe-Western Africa area.[87] Of the three repair ships, ACMA operates, two are based in Europe, one in Portland, UK and one in Brest, France. The Mediterranean Cable Maintenance Agreement (MECMA) covers the Mediterranean Sea, the Black Sea and the Red Sea. It has two cable ships based in La Seyne-Sur-Mer, France, and Catania, Italy.[88] This implies that three repair ships are based in the European Union. These, however, are in charge of a vast maritime area. The repair capacities are hence very limited.

Photo: Cable repair ship[89]

As we discuss in the following, each of the elements of the cable system is vulnerable to different attack scenarios.

[85] OFS Optics, 'What is Distributed Acoustic Sensing (DAS)?', n.d..
[86] D. R. Burnett, R. Beckman, and T. M. Davenport (Eds.), 'Submarine Cables. The Handbook of Law and Policy', 2013, p. 155.
[87] ACMA, 'Atlantic Cable Maintenance & Repair Agreement', n.d..
[88] Mediterranean Cable Maintenance Agreement (MECMA), n.d..
[89] Photo purchased from Ecorys on Shutterstock image database.

5.1.2 Modes of attack: Physical destruction

Several modes of attack on the cable infrastructure are thinkable. The most important are scenarios of physical destruction. This can either be of a single cable or a coordinated attack on several cable connections as well as landing stations and repair infrastructure.

Attacks on cables can be carried out in different ways. Firstly, by weaponizing civil vessels, including research vessels, fishing vessels, transport vessels or leisure yachts, and using improvised cutting devices (ICDs) such as anchors and dredging devices. Such forms of attack do not require technologically sophisticated capabilities, such as undersea capabilities, and are easy to implement, given that vessels can be hidden in common marine traffic. The main way of preventing such attacks is through surface surveillance of civil maritime activities and the identification of anomalous behaviour.

A second form of attack is through undersea explosives. These can be carried out by using military-grade naval mines or maritime improvised explosive devices (MIEDs) that can be remotely triggered. MIEDs, in particular, are easy to manufacture and cheap in production.[90] Considering the physical structure of the cables, already low explosive strength can interrupt a cable connection. Operating and placing mines require skills in handling explosives and minor undersea capabilities (divers). Preventing such attacks is more difficult and requires a combination of surface and undersea surveillance as well as mine-hunting capabilities to detect and destroy explosives.

The third form of attack is through submersible boats, crafts, or military-grade drones and submarines, which can be manned or unmanned. Submersible technology is increasingly widespread and readily available in the diving industry. Also, criminal organisations have reportedly been constructing and using submersible assets for smuggling operations.[91] This indicates that such technology is not only available to high capability naval forces. Submersible assets can be used to place mines and MIEDs and to employ higher-end technologies, such as self-propelled underwater weapons (torpedoes) and prospectively chemical or laser weapons. Submersibles are more difficult to detect and require sophisticated underwater surveillance infrastructure across the entire length of cables.

Another form of attack does not directly target the undersea cables but the broader infrastructure on land. Landing stations in which the undersea cable connects to the land are particularly vulnerable sites, with attack scenarios ranging from cutting power supplies to the detonation of improvised explosive devices to missile attacks. Such attacks are likely to imply significant damage and are difficult to repair in a short time.

A related potential target is the wider repair and maintenance infrastructure of cable ships and depots. As shown, only three cable ships are based in the European Union, with an additional one based in the UK. Ships and depots are vulnerable to the entire spectrum of weapons used on land (e.g. improvised explosive devices, missiles) and against marine vessels (MIEDs, torpedoes, missiles). Given the importance of the repair infrastructure, a concerted attack against cables and the regional repair ships is a scenario that would imply a significant outage of connectivity.

This indicates that attacks on the cable infrastructures can be low-cost operations that do not necessarily require high-end capabilities unless carried out exclusively on the underwater level. The planning and implementation of a major coordinated attack scenario to go unnoticed, however, implies considerable organizational capabilities in planning and coordination across different locations.

[90] S. C. Truver, 'Mines and Underwater IEDs in U.S. Ports and Waterways. Context, Threats, Challenges, and Solutions', *Naval War College Review*, *61*(1), 2009, pp. 1–12.
[91] J. Guerrero, 'Narcosubmarines. Outlaw Innovation and Maritime Interdiction in the War on Drugs', *Singapore: Palgrave Macmillan*, 2020.

As the data presented in chapters 3 and 4 indicate, a full EU wide blackout is highly unlikely given the number of cables and contingency available. It is, however, a theoretically possible scenario under conditions of an armed conflict. A coordinated attack on several cables, or a simultaneous attack on cables and the repair infrastructure could cause significant disruption. This is particularly the case for the vulnerable EU member states identified above and the islands and oversea territories, some of which rely on very limited cable connections.

5.1.3 Modes of attack: Data theft and intelligence

Another scenario, which is frequently mentioned in the media and elsewhere, concerns the tapping into cables to derive, copy or obfuscate data for intelligence purposes. Tapping the cables at sea is highly unlikely because it is technically challenging. According to observers, 'it is not publicly known whether any country is even capable of it'.[92] While technological capabilities exist in different forms, it is for pragmatic reasons that make tapping an unlikely scenario with a direct impact and suggest that this could be an exaggerated threat.[93] Moreover, attempts to tamper with a cable would most likely not go unnoticed by the cable operator, given that the majority of cables have surveillance to identify disruption. In consequence, the scenario of information theft, spying, and intelligence operations targeting cables at sea is rather unlikely.

Yet, multiple parts of the undersea cable supply chain can potentially be compromised, enabling the interception of data, surveillance, and traffic disruption. Cable building companies can potentially insert backdoors, install surveillance equipment, and place disruption triggers into the components of a cable before the cable is deployed. Pragmatically, onshore landing stations and facilities linking cables to terrestrial networks are more accessible and more vulnerable targets of spying and intelligence operations.

5.1.4 Modes of attack: Digital means

A third scenario concerns the use of cyber weapons to target the technical operability of the undersea cable infrastructure. There are numerous ways in which cyber-attacks can be carried out against the network. One of the most significant cyber threats is linked to the reliance on remote network management systems. As network management systems are often connected to the internet and rely on HTTP and TCP/IP protocols and non-proprietary software[94], they become susceptible to a range of cyber threats. Hacking into network management systems can provide attackers control of multiple cable management systems, visibility of networks and data flows, knowledge of physical cable vulnerabilities, and the ability to monitor, disrupt, and divert traffic.[95] Network Operation Centres, remote access portals, and other systems needed for the functioning of the cable network – such as electrical power, routers, heating, ventilation and air-conditioning – are also potential cyber-attack vectors.

The above scenarios document that there are significant opportunities to carry out attacks. In what follows, we conduct a threat analysis drawing on two key factors: capability and intent. We start by reviewing the threat from state actors with a focus on operations short of war. We then turn to an analysis of non-state actors.

[92] P. Morcos, and C. Wall, 'Invisible and Vital: Undersea Cables and Transatlantic Security', *Center for Strategic and International Studies*, 11 June 2021.
[93] O. Khazan, 'The Creepy, Long-Standing Practice of Undersea Cable Tapping', *The Atlantic*, 16 July 2013.
[94] Software that has no patent or copyright conditions associated with it.
[95] Public-Private Analytic Exchange Program (AEP), 'Threats to Undersea Cable Communications', *Department of Homeland Security*, 28 September 2017.

5.2 State-sponsored threats

Both the cyber and the maritime domains have increasingly become spaces of grey zone warfare and hybrid threats. The concept of grey zone and hybrid warfare refers to malicious activity below the threshold of armed conflict. Cyber and maritime lend themselves to such practice since the vastness of the spaces and the high number of diverse public and private actors involved make it more difficult to attribute attacks or damages and allow to blur the lines between state-sponsored and private activities. Due to the complexity of activities and sheer scale, they are moreover spaces that are very difficult to monitor and conduct surveillance, although significant technological progress is being made in these regards. Our analysis below focuses on two-state actors that are known to utilize grey zone tactics for political aims.

5.2.1 Russia

The Russian armed forces have undergone significant modernisation since 2008. This modernisation has been a key enabler for Russian revanchism in the former Soviet republics and increased military activism in the Middle East and Africa.[96] Upgrading the Russian Navy has been a key focus of the overall modernisation.[97] Special focus is set on the Yantar class intelligence ships and auxiliary submarines, both of which are able to disrupt undersea cable infrastructure. In addition, modern patrol boats, frigates, and destroyers are being deployed. According to a 2019 NATO report on North Atlantic security, 'these are all joined by new abilities to deploy mini-submarines by stealth, explore underwater sea cables, and exercise electronic-warfare jamming'.[98]

Observations of Russian submarine activities in territorial waters and in proximity to cable routes, which became public starting in 2015[99], continue to raise concerns that the Russian navy tampers with cables or cuts them as part of a hybrid warfare campaign. NATO officials have recurrently emphasised that there is unprecedented interest by the Russian navy in cable locations[100.] For instance, the commander of NATO's submarine forces in 2017 was cited as saying that '[w]e are now seeing Russian underwater activity in the vicinity of undersea cables that I don't believe we have ever seen' and continued by suggesting that 'Russia is clearly taking an interest in NATO and NATO nations' undersea infrastructure.'[101] NATO defence ministers expressed such concerns during a 2020 meeting.[102]

In January 2022, the UK's Chief of Defense alerted policymakers in an interview that the Russian undersea activities were unprecedented and directly targeted cable systems.[103] In February 2022, Russia conducted a naval exercise southwest of Ireland (just outside of Ireland's Exclusive Economic Zone), very close to several submarine data cables linking Britain, France, and the US. An Irish military source is quoted noting that 'the intention is not to cut the cables but to send a message that they can cut them anytime they want.

[96] H. Breitenbauch, and T. Liebetrau, 'Technology Competition, Strategic implications for the West and Denmark', *Djøf Publishing in cooperation with the Centre for Military Studies*, 2021, p. 54.
[97] R. Connolly, and M. Boulègue, 'Russia's New State Armament Programme, Implications for the Russian Armed Forces and Military Capabilities to 2027', *Chatham House the Royal Institute of International Affairs*, May 2018.
[98] N. Soames, 'Evolving Security in the North Atlantic', *NATO Defence and Security Committee (DSC), Sub-Committee on Transatlantic Defence and Security Cooperation (DSCTC)*, 13 October 2019.
[99] D. E. Sanger, and E. Schmitt, 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort', *The New York Times*, 25 October 2015.
[100] G. Hinck, 'Evaluating the Russian Threat to Undersea Cables', *Lawfare*, 5 March 2018.
[101] M. Birnbaum, 'Russian submarines are prowling around vital undersea cables. It's making NATO nervous', *The Washington Post*, 22 December 2017.
[102] A. Brzozowski, 'NATO seeks ways of protecting undersea cables from Russian attacks', *Euractiv*, 23 October 2020; NATO, 'Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers', 22 October 2020.
[103] Guardian (The), 'UK military chief warns of Russian threat to vital undersea cables', 8 January 2022.

The audience for that message is NATO, not Ireland.'[104] With the evolving war between Russia and Ukraine, this message is concerning. While neither Ukraine nor its neighbours are dependent on undersea cable infrastructures, since they primarily rely on terrestrial connectivity, the increasingly aggressive Russian undersea activity raises the possibility that Moscow could seek to damage cable networks as part of escalating the conflict through grey zone activities.

Russia has both experience and an interest in using unconventional or hybrid means of warfare, such as disrupting communications networks. In fact, during the Crimea annexation, Moscow severed the main terrestrial cable connection to the outside world to gain control of the peninsula's internet infrastructure and hence the flow of information. This enabled the Kremlin to spread disinformation and promote its actions as legitimate.[105]

There are hence several imagined Russian objectives severing a cable. These include damaging cables in operations short of war blocking military or government communications in the early stages of a conflict, shutting down internet access for a targeted population, sabotaging an economic competitor, or causing global disruption for strategic purposes. These acts can be either pursued individually or simultaneously.

5.2.2 China

In recent years, infrastructure companies with strong ties to the Chinese state have significantly increased their construction and ownership of undersea cables. HMN Technologies (formerly Huawei Marine Networks) has a global market share of about 10 % and built or repaired almost 100 of the world's 400 submarine cables.[106] The investment in the cable infrastructure is integral to the Chinese Digital Silk Road (DSR) project. The DSR was introduced in 2015 by an official Chinese government white paper as an important component of Beijing's Belt and Road Initiative (BRI).[107] With the ongoing digital trade war, the growth of the Chinese tech sector, and the sharpened focus of DSR, Chinese leaders will likely continue to leverage national technology companies for geopolitical purposes, including an aim to build, connect, and control digital technology infrastructure throughout the globe.

Deciding where, when, and how to build undersea cables not only provides the companies, and thereby the Chinese state, with an increasing power to shape global internet traffic, but it also enables data interception and development of technological dependence. In addition, the cable owners might insert backdoors into or otherwise monitor cables and landing stations. Similarly, cable builders can compromise the security of the physical infrastructure along the ocean floor. As China exerts increasing control over the cable infrastructure, the risk of undermining security and resilience grows.

In August 2020, the US announced the Clean Network Program, which includes five lines of effort –in addition to 5G – to counter China's influence on US telecommunication networks, mobile app stores, software apps, cloud computing, and undersea cables.[108] Before that, in June 2020, the US Justice Department objected to a Google and Facebook project to install an undersea cable from the US to Hong Kong. The Justice Department raised concerns that Beijing could use its new national security law to access cable data on the Hong Kong side.[109] According to a US expert, 'the US government highlighted the risk of Chinese state influence on two fronts: compromising cable data via cable owners (e.g., intelligence

[104] C. Gallagher, and S. Carswell, 'Russian naval drill to still take place over vital cables, experts believe', *The Irish Times*, 31 January 2022.
[105] J. Sherman, 'Cord-cutting, Russian style: Could the Kremlin sever global internet cables?', *The Atlantic Council*, 31 January 2022.
[106] A. Bergin, and S. Bashfield, 'Digital age lies vulnerable to threats from underwater', *Australian Strategic Policy Institute*, 18 October 2021.
[107] H. Shen, 'Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative', *International Journal of Communication*, Volume 12, 2018, pp. 2683-2701.
[108] U.S. Department of State, 'The Clean Network', n.d..
[109] J. Sherman, 'The US-China Battle Over the Internet Goes Under the Sea', *Wired*, 24 June 2020.

collection through a state-controlled landing point) and changing the Internet's physical shape to route more global traffic through China (e.g., creating more chokepoints in the global network under the Chinese government's control)'.[110]

China has also been accused of using sand-dredging as a weapon against Taiwan in a campaign of grey-zone warfare. Chinese dredgers have been observed swarming around the Matsu Islands, dropping anchors and scooping up vast amounts of sand from the ocean bed for construction projects in China. However, 'Taiwanese officials and Matsu residents say the dredging forays have had other corrosive impacts - disrupting the local economy, damaging undersea communication cables and intimidating residents and tourists to the islands.'[111]

In addition, China holds the military capabilities to inflict great damage on the undersea cable network by sabotaging or destroying one or more cables. However, the Chinese deployment of its increasing maritime military power to sabotage or destroy one or more undersea cables is not likely to take place outside the context of existing tensions in the Indo-Pacific. Therefore, the potential immediate impact on Europe's security is more limited. Yet, in the light of the broader engagement of the EU in the Indo-Pacific and concerns over grey zone activities, it is arguably a growing concern.

5.2.3 Other states

A number of other states are known to develop and employ grey zone tactics at sea, including the use of research and fishing vessels as well as coast guard patrol crafts for such purposes. Reports indicate that North Korea, Iran, Israel, and Turkey have employed such tactics in the maritime sphere as part of militarized interstate disputes.[112] This shows intent in broad terms, and these states also have the required capabilities. Such activities have so far occurred in the Mediterranean and the Strait of Hormuz primarily. No cases that involve undersea data cables have been reported so far. The threat scenarios and their impact on Europe security are limited.

A related scenario is the escalation of civil war and its (intentional or unintentional) spill over into the maritime domain. Here, the conflict in Yemen needs to be considered as a potential threat. The subsea off the coast of Yemen is one of the major data highways of the Europe-Asia cable system, passing through the Red Sea. Reports indicate that the conflict in Yemen has had an impact on shipping activities and maritime security in the area.[113] This included the use of naval mines and divers. Hence, there is a risk that the conflict will lead to the damage of undersea data cables as part of such activities. Overall, political instability in the vicinity of cable routes needs to be seen as a significant risk to resilience.

5.3 Threats emanating from non-state actors

5.3.1 Violent extremism and maritime terrorism

Terrorist organizations have shown the will and capability to target critical infrastructures in the past. However, the majority of such attacks have aimed at a high number of victims and maximizing publicity rather than targeting the digital economy or financial markets directly.

[110] J. Sherman, 'Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security', *Atlantic Council*, 2021, p. 12.
[111] Y. Lee, 'China's latest weapon against Taiwan: the sand dredger', *Reuters*, 5 February 2021.
[112] J. Goldrick, 'Grey zone operations and the maritime domain', *The Strategist,* 30 October 2018; A. Singh, 'Deciphering Grey-Zone, Operations in Maritime-Asia', *Observer Research Foundation*, 2018; F. Nadimi, 'Iran and Israel's Undeclared War at Sea (Part 2): The Potential for Military Escalation', *The Washington Institute for Near East Policy*, 13 April 2021; L. Will, 'Conflict in the Eastern Mediterranean: Turkey Clashes with Neighbors Over Offshore Gas Reserves', *The Yale Review of International Studies*, November 2020.
[113] E. Ardemagni, 'Red Sea Security: How Yemen Tests The "Abraham Equation"', *Italian Institute for International Political Studies*, 15 December 2021.

The limited resources and capabilities required, e.g. by using MIEDs to harm cables or target landing stations, imply that the risk of a terror attack exists. While a successful attack against one or more cables can do harm and draw publicity, terrorist organizations themselves rely on digital infrastructures. An attack that takes out digital infrastructure (and hence the capacities to self-organise, but also the ability to reach wide publicity) should not count as a primary objective of such activities.

While a full blackout scenario within the EU or one of its Member States is very unlikely, the evaluation changes in terms of small European islands, oversea territory, oversea bases, and other external targets. The Western Indian Ocean, for instance, is a region where terrorist attacks have occurred in the past, and extremist organisations are particularly active, like maritime and terrestrial incidents in Djibouti, Mozambique, Maldives, Somalia, Kenya, Sri Lanka and Pakistan document.[114] This raises the possibility that attacks on undersea cables could be carried out in order to harm the naval bases of Member States in Djibouti or Bahrain that are vital for running the current naval operations in the region (e.g. the EU Naval Force Operation Atalanta or the European Maritime Awareness Strait of Hormuz operation (EMASOH). Also, the French overseas territories of La Reunion and Mayotte might be at a higher risk, not the least in light of their weaker connectivity. The Red Sea and the political situation in Egypt as one of the bottlenecks in the EU's connectivity to Asia also require attention since they are known operational terrain of radical organizations.[115]

5.3.2 Criminal organisations

Transnational criminal networks are known to heavily use digital infrastructure for running their operations and as a key avenue to commit cybercrime, for instance, through ransomware.[116] This makes it likely that transnational criminal networks seek opportunities to exploit the vulnerabilities of the undersea cable network. Experts from the UN Office on Drugs and Crime's Global Maritime Crime Programme, for instance, have highlighted that criminals might exploit the vulnerability of cable infrastructures.[117] While no incidents have been publicly reported, two scenarios need consideration.

The first scenario is that a criminal organisation threatens to destroy cable infrastructure and demands a ransom. The difficulties linked to detecting threats, such as from MIEDs and submersibles and their availability, make a ransom scenario towards a cable operator, a state or an overseas territory with weak cable links likely. Detecting the threat can easily take weeks, and a ransom payment could be a valuable option for the targeted actor in such a scenario. This could create a potentially dangerous precedent for such a criminal business model if the information on the incident is not shared widely across operators and states. Encouraging reporting and information sharing across industry and police will be hence vital.

A second scenario of criminal use is that an attack might occur to cover up other criminal activities. Damaging the cable network could be beneficial to prevent surveillance and conduct a major smuggling operation, conduct a black-market transaction, or as a distraction in another form of cybercrime.

5.3.3 Synthesis

At the time of writing, there are no publicly available and verified reports indicating deliberate attacks on the cable network by any actor, be it Russia, China, or a non-state group. The large-scale scenarios of a complete loss of connectivity underpinning most threat discourse thus seem to be built not on prior incidents but on overall assessments of the geopolitical and threat landscape. Arguably, this implies that

[114] See: C. Bueger, and J. Stockbruegger, 'Maritime security and the Western Indian Ocean's militarisation dilemma', *African Security Review*, 2022 doi: 10.1080/10246029.2022.2053556.
[115] Institute for Economics & Peace, 'Global Terrorism Index 2020: Measuring the Impact of Terrorism', 2020.
[116] A. M. Bossler, and T. Berenblum, 'Introduction: new directions in cybercrime research', *Journal of Crime and Justice*, *42*(5), 2019, pp. 495-499.
[117] I. Ralby, 'Briefing on Undersea Cables Expert Meeting', *Vulnerabilities to Undersea Data Cables*, UNODC, January 2019. .

the threat scenarios being discussed could be exaggerated and suggests a substantial risk of threat inflation and fearmongering.

However, many countries and non-state actors possess the power to inflict harm on the submarine cable network, and reports and scenarios indicate that this has to be a major concern. In addition, acquiring the capability to cause harm to the cable network comes at a low cost. This implies that the scenario of a smaller scale attack, in which one or several cables are attacked for symbolic reasons, e.g. to demonstrate capability and intent, is plausible.

Considering the risk of deliberate attacks on cable networks, several motives can be imagined. Should the geopolitical tensions between the West and Russia continue to increase, the latter might consider causing symbolic damage to the cable network as part of an act of provocation. The prospect of holding a financial transaction hostage or destroying it could encourage a terrorist organization to attack the cable network. Transnational criminal networks could exploit the vulnerability of the network. In those scenarios, European countries are likely to feel the direct consequences. Assigning these motives and their likelihood is, however, at current a speculative exercise.

6 Member state awareness and responses

6.1 Overview and legal status

As chapters three and four have indicated, not all EU member states are equally important for the system and depend differently on undersea data cables. A substantial number of countries rely primarily on terrestrial connections and are hence indirectly dependent on subsea cables provided by other states. Five EU Member states are landlocked countries (Austria, Czech Republic, Hungary, Luxembourg, Slovakia), while a series of other states are not major connection points to the undersea cable network (e.g. Belgium, Bulgaria, Croatia, Germany, Lithuania, Latvia, Netherlands, Poland, Romania, Slovenia). However, all of these countries are dependent on subsea cable connections for their cross-continental internet traffic.

In the following, we rely on an empirical study of selected member states which are vital in the EU's digital undersea connectivity. The analysis includes three key connecting states: (1) Denmark, which has a substantial number of cable connections to North America, (2) France and (3) Italy, which are the key landing destinations for cable connections to Asia. (4) Portugal and (5) Spain, which are vital for connectivity to the South Atlantic region (South America and Africa). These five Member states also have significant autonomous overseas territories. In addition, we also include two EU island states in the discussion. (6) Malta and (7) Ireland are fully dependent on subsea cables and cannot rely on redundancy through terrestrial connections. In addition, we consider (8) Estonia as one country known to be a pioneer in digital policies and a post-Soviet state with potential immediate exposure to threats from Russia.

We structure our discussion in two dimensions: 1) Awareness and strategic responses: What indications are there about the level of awareness in the EU Member States and their strategy processes? 2) Monitoring and Governance: How are cable protection and resilience currently governed, and how is the relation between different relevant actors organised? We conclude with a discussion on how far the current models hold more general lessons or promising practices.

6.2 Strategy and awareness

There is a significant difference in Member State awareness and strategies concerning subsea data cable protection. In some Member States, there is considerable political awareness. The issue is within public debates in these countries and featured in national security and defence strategies, predominantly those that focus on maritime and cyber security. In the other Member States, public and political awareness is very limited, and data cable protection is absent from national security strategies and policy and addressed as a primarily technical or self-regulatory issue.

A key determining factor appears to be whether countries have been exposed to Russian subsea activity and whether they posit significant naval underwater capabilities. Such countries tend to express higher awareness and identify cable protection as a primarily military issue. Three Member States document high-level military awareness in this regard: France, Ireland, and Portugal. In all three states, military leadership went public concerning the issues, or the issue has been discussed in the national media.

The issue is significantly discussed within French naval strategy and national discourses. The 2017 French Strategic Review of Defence and National Security states that 'Maritime spaces are at the heart of growing tensions, because of their central role in the globalization of flows of all kinds, including digital ones (submarine cables), the resources they contain and the development of naval and air strike capabilities working at distance.'[118] This was reiterated in the 2021 Strategic Update released by the Ministry of Defense, which stresses that 'The seabed is also increasingly becoming the setting for power struggles

[118] République Française (La), 'Revue stratégique de défense et de sécurité nationale', 2017, p.43.

(seabed warfare), with the key issue of submarine cables in particular.'[119] The French Ministry of Defense hence published a national strategy for controlling the seabed in February 2022.[120] At the moment, the fear of Russia shutting down the internet in Europe draws a lot of attention in France.[121]

While Ireland does not possess significant subsea surveillance capabilities, relevant Russian subsea and intelligence activities have been reported several times in national and international media outlets, creating high-level awareness of the threat.[122] The government launched a public consultation on 'International Connectivity for Telecommunications' in 2020, where the issue of cable security became a concern.[123] In a 2021 parliamentary debate, the issue was raised, and it was discussed whether and how cable security is a key gap in Irish defence policy.[124] The Report of the Commission on the Defense Forces tasked to provide a review of Irish defence capabilities published in February 2022 flags the issue and calls for enhancing the sub-surface capabilities of the Irish Naval Service in order to allow it 'to monitor activity in the vicinity to sub-sea cables'.[125]

Portugal has been exposed to Russian naval activities at least since 2014, when a Russian hydrographical vessel was intercepted south of the port of Faro.[126] Russian naval activities have since been an ongoing concern in the country and for military leadership.[127] Portugal has been heavily investing in cable infrastructure as part of its digital economic policy and has also taken leadership in this regard on an EU level as part of its 2021 European Council presidency in promulgating the 'European Data-Gateway Platforms Strategy', which would see the EU become a leading global data manager and digital service provider.[128] The high-level governmental priority for subsea cables is also reflected in the work of the Portuguese navy, which has identified subsea cable protection as a priority with a focus on the Atlantic region and has advocated for considering the theme in the Strategic Compass and refreshing the EU Maritime Security Strategy.

Given their vicinity to Russia and exposure to foreign naval activities, both Estonia and Denmark are an outlier. Both countries do not possess significant subsurface naval capabilities and show a lack of awareness. The Estonian navy has frequently issued concerns about Russian naval and intelligence behaviour,[129] and also in Denmark, such observations gained some publicity both with an eye on the Atlantic and the Baltic region.[130] Surprisingly, this has not led to any substantial public debate on subsea cables nor any publicly available strategic processes or concerns about the threat to digital connectivity in the two countries. This indicates that the level of awareness in both countries is relatively low.

A different situation arises with regards to the Mediterranean countries. In the public debate in Italy, Spain and Malta, threats to the data cables have not featured prominently, nor are foreign naval activities considered a priority, given that most of the attention is devoted to the problem of irregular migration

[119] République Française (La), 'Actualisation Stratégique 2021', 2021, p. 18.
[120] République Française (La), 'French Seabed Strategy', 2021.
[121] e.g. J. Pousson, 'Guerre en Ukraine : la Russie peut-elle vraiment couper Internet en Europe?', *Le Parisien*, 4 March 2022; V. Geny, 'La Russie peut-elle priver l'Europe d'Internet en sabotant des câbles sous-marins?', *Marianne*, 5 March 2022; S. Besanger, 'La Russie peut-elle vraiment priver l'Europe d'internet en coupant les câbles sous-marins?', *Ouest France*, 9 March 2022.
[122] S. Ankel, 'Russian intelligence agents reportedly went to Ireland to inspect undersea cables, and it's reigniting fears they could cut them and take entire countries offline', *Business Insider*, 17 February 2020.
[123] A. Whittaker, 'Connected Ireland: How subsea fibre optic cables help to drive our social, economic and industrial development', *Engineers Ireland*, 13 November 2020.
[124] J. Mooney, 'Ireland unable to protect subsea cables from Russian attack', *The Times*, 25 November 2021.
[125] Commission on the Defence Forces, 'Report of the Commission on the Defence Forces', 2022.
[126] BBC, 'Portugal navy escorts Russian ship away from coast', 5 November 2014.
[127] Portugal News (The), 'Portugal's navy keeps watchful eye as Russian war fleet cruises past coast', 26 January 2017.
[128] L. Cerulus, 'Lisbon eyes undersea cable investment to bolster EU tech infrastructure', *Politico*, 10 December 2020.
[129] S. Sprenger, 'Estonian intelligence flags Russian civilian vessels as would-be spy ships', *Defense News*, 13 March 2019.
[130] S. Nyboe McGhie, 'Efter 15 år i blinde under havoverfladen: Nu skal Danmark igen jagte russiske ubåde', *Berlingske*, 6 December 2019.

across the Mediterranean. Both Italy and Spain indicate basic governmental awareness of the issue, and subsea cable infrastructure is mentioned in the relevant national security and ocean policy documents. Spain issued a dedicated maritime security strategy in 2013 and listed the protection of marine infrastructures as one of the priorities.[131] Italy includes subsea cables in its national security policy framework for critical infrastructure protection.[132] In 2019, the Italian Navy (Marina Militare) published an updated version of its 2019-2034 Strategic Planning which outlines the future composition of its fleet and assets.[133] The strategy underlines the Navy's responsibility for protecting critical undersea infrastructure.

None of the examined Member States has so far laid out a policy or strategy that exclusively concerns subsea data cable protection. However, the investigated Member States all have governance frameworks in place, which is the issue we turn towards next.

6.3 Governance arrangements

EU Member states have developed quite different national frameworks for subsea cable resilience. These divergences primarily result from 1) the general level of awareness and priority assigned to cable infrastructure and 2) the general organisation of law enforcement in the maritime space. In our investigated sample, three key prototypical models come to the fore. Firstly, national security-driven arrangements as provided in the cases of France and Portugal; secondly, civilian-led arrangements as most prominently provided in the case of Malta. Thirdly, industry-led self-regulatory arrangements as best visible in the case of Denmark. We discuss each model with a focus on how these arrangements organise information sharing and surveillance as well as repair and responses. However, each of these models needs to be understood as simplification and against the backdrop of a substantial policy-centric governance structure. As we discuss in the concluding section, in each of the models, the industry has a high level of independence, and self-regulatory processes are key background drivers.

States that prioritise inter-state threats tend to favour national security and navy-led models. In France, the Secretariat-General for National Defence and Security, an inter-ministerial organ under the Prime Minister of France, plays an important role in ensuring and coordinating the national security perspective of subsea cable protection, while the Secretariat Général à la Mer (SGMer) are central for coordinating administrative tasks related to data cable protection. In addition, the French Navy plays an important role in protecting cable installations in French waters in collaboration with private companies. In France, companies such as Orange Marine and Alcatel Submarine Network, which are world leaders in laying and maintaining submarine cables, 'ensure regular checks themselves to detect and locate any cuts or damage'.[134] A range of other French public authorities also have a stake in undersea cable protection such as L'agence nationale de la sécurité des systèmes d'information (ANSSI), État-Major des armées (EMA), Ministère de l'Europe et des Affaires étrangères (MEAE) and Direction générale de la Sécurité extérieure (DGSE).

A good example of a civilian-led model is Malta. In the country, cable protection is coordinated by a dedicated Critical Infrastructure Protection (CIP) Directorate, which falls within the Ministry for Home Affairs, National Security and Law.[135] The directorate is the key authority conducting surveillance and is also in charge of cyber security monitoring. It hence offers an example of a sole lead authority that combines maritime and cyber security. The directorate collaborates closely with the local communications regulator, the Malta Communication Authority (MCA). The CIPD and the MCA collaboration is formally

[131] I. J. García Sánchez, 'Analysis of the National Strategy for Maritime Security 2013. Prosperity and Welfare beyond the Coastline', *Instituto Español de Estudios Estratégicos*, 10 December 2013.
[132] T. de Zan, G. Giacomello, and L. Martino, 'Italy's Cyber Security Architecture and Critical Infrastructure', in *Routledge Companion to Global Cyber-Security Strategy*, 2021.
[133] Stato Maggiore della Marina, 'Marina Militare Linee di Indirizzo Strategico', *Rivista Marittima*, 2019.
[134] L. Lagneau, 'Comment la Marine nationale surveille les câbles sous-marins de communication?', *Zone Militaire*, 11 December 2018.
[135] Established in accordance with Article 3 of Legal Notice 434 of 2011 and Council Directive 2008/114/EC of 8 December 2008.

embedded in national legislation, namely Legal Notice 216 of 2018. The directorate liaises closely with the cable operating industry, which includes site visits and inspections of cable locations. The digital industry is obliged to cooperate closely in breakdown scenarios. The Armed Forces of Malta only have a minor role but can be requested to assist the CIP Directorate and the cable industry in patrolling and surveillance and as a first responder. This model is noteworthy considering that it provides a well-organised process. However, Malta only has a very limited number of cables to protect.

The case of Denmark provides a good example of industry-led self-regulatory arrangements. In Denmark, the Danish Coastal Authority regulates the laying of cables,[136] and The Danish Maritime Authority regulates the establishment of protection zones to avoid trawl and anchoring.[137] However, the surveillance and protection of the subsea cable network are primarily left to the private company cable owners and operators. They provide the basic level of security for the submarine cable network by, e.g., installing monitor and surveillance systems, addressing cable failures by conducting investigations, and filing cases when human actors are damaging cables. In addition, the Danish Cable Protection Committee (DKCPC), an association of gas, telecommunication, and electricity companies, which own or operate submarine cables and pipelines in Danish maritime territory, works to improve protection. The DKCPC raises awareness, enables stakeholder meetings, and facilitates information sharing. Moreover, the DKCPC collaborates with the Royal Danish Navy's 'Joint Rescue Coordination Centre, MAS – Marine Assistance Service'. According to the DKCPC, the Danish Navy does, however, not engage with the industry in proactive protection, surveillance, or law enforcement efforts around subsea data cable protection.

6.4 Synthesis: Promising practices?

The analysis indicates that a minimum awareness and governance processes are present in EU Member States. Yet, it also demonstrates significant differences. The key driver in terms of awareness is whether or not there is attention to a potential Russian threat and whether such concerns are taken seriously by national navies. In such cases, undersea cables are an explicit concern. The other countries include loose references to subsea infrastructure in their national documents and strategies but do not foreground the importance of cables. The reconsiderations of the threats from Russia following the 2022 Ukraine war indicate that attention in EU Members States is clearly on the rise.

Cable protection is a cross-cutting issue that spans a broad range of governing bodies. It concerns questions of military-civil relations, the relation between maritime and cyber security, but also how EU Member States have organised their maritime governance system, and how many agencies are involved. While all countries struggle with the problem of the high number of agencies involved, we have identified three different models with each different weaknesses and strengths. The navy-led model appears to face the problem of not adequately considering cooperation with the industry. The industry-led model appears not to allow for sufficient contingency and emergency planning. The civilian-led model seems to be the most integrative, but it is questionable how well it would work in countries with larger territorial waters and more complex maritime governance systems.

It is striking that many EU Member States largely forget the national security and geopolitical implication of the undersea cable network. Moreover, the subsea data cable infrastructure's significant impact on international information flows, security, and the economy is rarely engaged by European States. However, the growing awareness of the issue of cable protection also indicates that opportunities exist for improving awareness, governance mechanisms, and resilience within existing Member State structures and agencies.

[136] Danish Government, 'Bekendtgørelse af lov om kystbeskyttelse m.v.', 29 May 2020.
[137] Danish Government, 'Bekendtgørelse om beskyttelse af søkabler og undersøiske rørledninger', 27 November 1992.

7 EU level awareness and activities

The EU institutions have so far not laid out a policy, strategy, initiative or programme that would primarily and explicitly concern data cable protection. However, subsea data cable infrastructure is a concern within several ongoing EU policy processes, where the issue has different priorities. At least five policy fields and the related institutions are of relevance. Questions of cable security are most explicitly addressed in 1) maritime security and 2) cyber security policy. In more remote terms, subsea cables are also issues within 3) ocean governance and 4) digital and infrastructure policy. Moreover, they are a critical component in 5) external action, including development policy and security and defence policy.

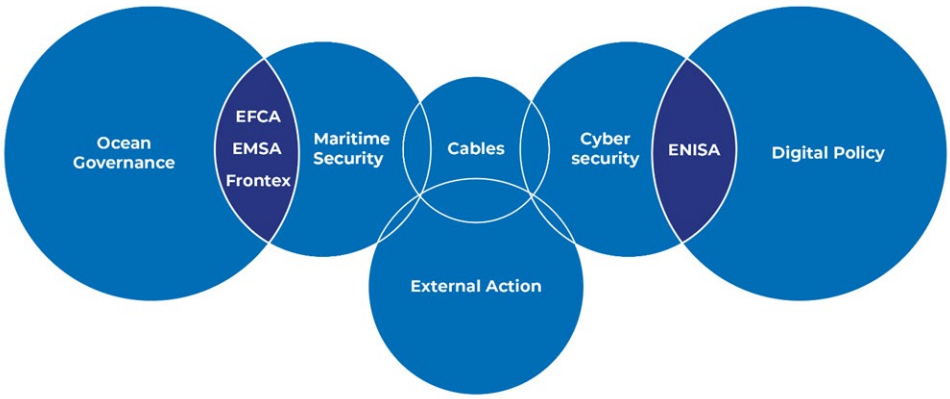

Figure 5: Undersea cable relevant EU policies and agencies

These are areas in which the protection and resilience of the data cable infrastructure is a concern but not necessarily a priority. Moreover, each area is cross-cutting and complex in its own right and involves diverse institutional dynamics. The mandate of several EU technical agencies is relevant, although none of them is explicitly tasked to address data cable protection and resilience: This includes European Border and Coast Guard Agency (Frontex), European Defense Agency (EDA), European Environmental Agency (EEA), European Fishery Control Agency (EFCA), European Maritime Safety Agency (EMSA), and European Union Agency for Cyber Security (ENISA).

Our review below of the relevant policy processes and technical agencies indicates firstly that a minimum awareness across the EU and its agencies is present. Secondly, it demonstrates that there are ample opportunities for addressing cable resilience within existing frameworks and agencies. This in particular concerns coordination, information sharing and surveillance. Yet, thirdly, there is a high risk that cable resilience remains at the margins of policy discourses, and no agency is claiming immediate responsibility or authority since it sits at the intersection of different policies, mandates and directorates. However, the 2022 Ukraine crisis has brought new attention to potential threats and vulnerabilities in Europe. This includes new levels of public attention to the subsea cables.[138]

7.1 Maritime security

Maritime Security has been a key concern at EU level since the late 2000s. While initial attention was primarily on different expressions of crime at sea, particularly piracy and human smuggling, broader challenges were increasingly recognised. This led to a holistic understanding of maritime security, as exemplified in the adoption of the European Union Maritime Security Strategy (EUMSS) and its accompanying action plan in 2014.[139] The EUMSS offers a holistic outlook on different security challenges

[138] S. Seibt, 'Threat looms of Russian attack on undersea cables to shut down West's internet', *France24*, 23 March 2022.
[139] Council of the European Union, 'European Union Maritime Security Strategy, 11205/14', 24 June 2014.

at sea and, in particular, calls for risk analyses, resilience measures, and intra-European information sharing. In its summary of strategic maritime interests, the strategy emphasises the protection of critical maritime infrastructure and seabed cables against risks and threats.[140] This makes cable protection de facto a standing item on the EU's maritime security agenda. However, it is not an item that has been prioritised in the action plans and their implementation – in particular, vis a vis other maritime security challenges, such as piracy, people smuggling, or environmental protection.

7.1.1 EUMSS actions and their implementation

The lack of prioritization becomes clearly visible in a review of the action plans and their implementation reports. The 2018 revised action plan[141] lists the protection of telecommunication networks and sensors, including underwater, as one of its actions in risk awareness and management under the responsibility of the Member States, Commission, EEAS, and EDA to increase resilience (Action A.4.1). It calls for conducting common risk analyses (Action A.4.3).

The Action Plan also calls for 'cross-sectoral maritime security training and exercises' in which 'cyber-security and protection of critical maritime infrastructure, including submarine cables', is one of the priority areas (Action A.5.1). It emphasises the role of EMSA, Frontex and EFCA in this regard. The protection of subsea cables is moreover explicitly referred to in the regional actions on the North Sea and Baltic Sea, where the Action Plan calls for joint risk assessment and management exercises as well as 'regular data sharing' among EU Member States (B.5.1).

By contrast, the 2020 Report on the implementation of the revised EU Maritime Security Strategy Action Plan[142] fails to report on data cables explicitly. It loosely refers to Member State measures to consolidate the resilience of critical maritime infrastructure overall, with a focus on ports, maritime installations, and in particular, their cyber security (2.4.A), as well as efforts to improve information sharing between EFCA, EMSA, Frontex and the Member States, for instance, through the Common Information Sharing Environment (CISE). No dedicated activity with the objective of data cable resilience is reported, an evaluation that is confirmed in our review of agency activities below.

7.1.2 The EU's maritime agencies

EFCA, EMSA and Frontex are the three technical agencies that are key in EU maritime security and together provide surveillance, information sharing, and law enforcement coordination functions, also known as coast guard functions. Their mandate and focus differ:

EFCA is in charge of fishery regulation and supports EU Member States in surveillance of fishing activities, inspections, compliance and information sharing. EFCA's mandate is relevant considering that one of the main threat scenarios stems from fishing vessels. Interviews indicate a high level of awareness at EFCA that fishery is a core factor in data cable protection. However, it was pointed out that cable protection and surveillance are not explicitly an element in fishery policies and fishery compliance measures. Yet, the issue had been discussed at coast guard forums in which EFCA participates (discussed below).

EMSA is the EU's authority to assist member states in matters of marine safety. On the one side, this involves support for ensuring compliance with international and European safety regulations in ports and on ships. This includes directly security-related measures, such as the International Ship and Port Facility Security (ISPS) Code that was introduced as part of the response to international terrorism. EMSA's second key function is to monitor maritime activity with a focus on European waters but with global capabilities.

[140] EUMSS, IVc
[141] Council of the European Union, 'Council conclusions on the revision of the European Union Maritime Security Strategy (EUMSS) Action Plan 10494/18', 26 June 2018.
[142] European Commission, 'Joint Staff Working Document. Report on the implementation of the revised EU Maritime Security Strategy Action Plan, SWD (2020) 252', 23 October 2020.

EMSA develops a maritime situational picture for EU Member States and the other technical agencies. The picture is based on the Automated Identification System (AIS) that allows identifying the position and route of ships as well as satellite images derived from the Copernicus system. EMSA fuses such spatial data and provides algorithms that allow for the identification of suspicious and non-compliant behaviour which are used in maritime law enforcement operations. EMSA is also the lead agency in developing the Common Information Sharing Environment (CISE), which is intended to become the key tool for sharing maritime surveillance information across the EU by 2023. Given the substantial maritime surveillance capabilities that EMSA has developed, these provide established platforms that can be used to conduct surveillance of marine surface activities in strategic cable locations. Interviews indicate awareness of EMSA that its tools could be employed in such a way but that the agency so far does not have the mandate or staffing that would be required. EMSA's mandate is currently under review by the Commission, with DG MOVE in the lead.

Frontex's primary attention is preventing irregular migration and maritime crimes such as smuggling. It is the only maritime EU agency that has substantial law enforcement capabilities. These capabilities so far are fully focused on border protection. Frontex is in charge of the European Border Surveillance system (EUROSUR). EUROSUR integrates different assets (drones, aircraft, radar, etc.) to develop a shared maritime picture to prevent cross-border crime and irregular migration.[143] Each EU Member State contributes to the system through a dedicated national centre, with Frontex being responsible for fusing such data, including sources provided by EMSA. Frontex also operates the Maritime Intelligence Community & Risk Analysis Network (MIC-RAN). Set up in 2018, it is a network for the exchange of information, intelligence, cross-border crime statistics, and the dissemination of its risk analysis products. The MIC-RAN network is designed to support: 'operational/strategic early warnings, risk alerts, risk profiles, overview reports, area/port analysis, and mapping of EU/regional maritime risks.'[144] Since it intends to prevent and monitor transnational threats, this capability could also be employed to address cable resilience. Interviews indicate that awareness of cable resilience is low in the organisation and that the protection of critical infrastructures is interpreted to be outside of the agency's mandate.

Since 2018, the three agencies have started to explore how they can better cooperate in information sharing and risk management. This, in particular, has entailed awareness and harmonization of different types of data and methodologies used by each agency as well as the development of a joint glossary of terms. The CISE structures provide the key future architecture for strengthening the cooperation between the agencies in terms of information sharing and fusing and disseminating information from Member States.[145]

7.1.3 Coast guard forums

Coast guard forums are another vital tool in maritime security provision, information sharing and coordination across EU organs and Member States. The European Coast Guard Functions Forum (ECGFF) is the key entity within the EU, while a set of regional forums are important in the coordination with the EU's maritime neighbours. This includes the Mediterranean Coast-Guard Cooperation Forum, Baltic Sea Region Border Control Cooperation, the North Atlantic Coast Guard Forum (NACGF) and the Arctic Coast Guard

[143] European Commission, 'Report from the Commission to the European Parliament and the Council on the evaluation of the European Border Surveillance System (EUROSUR), COM (2018), 632', 12 September 2018.
[144], European Commission, 'Joint Staff Working Document. Report on the implementation of the revised EU Maritime Security Strategy Action Plan,. SWD (2020) 252', 23 October 2020, p 27.
[145] European Commission, 'Commission Staff Working Document. Review of the Common Information Sharing Environment (CISE) for the maritime domain: 2014 – 2019, SWD (2019), 322', 5 September 2019.

Forum (ACGF). Reportedly these regional forums, which are not formally EU entities, have discussed the question of cable security.

The ECGFF is an informal EU coordination mechanism that was created in 2009. It brings together over 30 national coast guard authorities from EU countries and associated Schengen countries to enable 'coordination of work on specific aspects, such as maritime information sharing, cyber-security, analysis of risks at sea and capacity building'.[146] While documents indicate that maritime surveillance and information sharing is the bulk of the work of the ECGFF, interviews indicate that the issue of cables has been flagged in past presentations, implying a general awareness of the issue among EU coast guard function agencies. However, the ECGFF has not explicitly turned cable protection into the main focus area. As the report of the implementation of the EUMSS indicates, the ECGFF is a very agile forum and has addressed cyber security in the maritime domain substantially. This was done through a series of workshops and a dedicated working group of both governmental and private stakeholders.[147] Since it has proven its capacity to address novel issues involving a high number of actors, it could also provide a useful forum for cable resilience.

The related European Coastguard Function training network is a mechanism coordinating the work of training academies in the field. Established to develop joint curricula and joint understandings of the essentials of coastguard operations, it serves as a potential supporting mechanism for both the work of ECGFF but also more broadly. So far, it has not developed course content that would address submarine dimensions but could be a viable way to enhance awareness.

7.2 Cyber security

Cyber security policy is the second key policy domain of relevance. In the past decade, cyber security has risen to the top of the political agenda in the EU, with cyber security elements having been integrated across several EU policy areas. Under the Commission Presidency of Ursula von der Leyen, the preeminent position of cyber security has been confirmed. In her political guidelines, Von der Leyen underlined that 'cyber security and digitalisation are two sides of the same coin. This is why cyber security is a top priority.' [148]

The first EU cyber security strategy was released in 2013. It is key to the strategy that the EU takes action 'to counter cyber risks and threats having a cross-border dimension' by strengthening European cyber resilience.[149] The strategy came along with the first-ever proposal for EU cybersecurity legislation – the network and information security directive (NIS-directive) adopted in 2016 to be fully implemented by member states in 2018.[150] 2017 saw an updated EU cyber security package. It included suggestions to

[146] European Commission, 'Coast guard cooperation', n.d..
[147] 'Because of the increasing cybersecurity challenges to both governmental and private stakeholders in the maritime domain, cybersecurity requirements are widely integrated in new capability projects and regulations. Ensuring sufficient levels of cybersecurity is considered even more essential following the introduction to the maritime domain of emerging technologies such as autonomous vessels, blockchain, remotely piloted systems, and the internet of things. Close coordination among key stakeholders at national level enables harmonisation of requirements and consistency in approaches (IT, LT, PT, RO). The ECGFF working group on cyber-attack prevention has also been an important platform for cooperation between MS seeking to develop common detection procedures and build a European network to fight cyber threats. Several countries (IT, BE, HR, PT, FI, ES) and EU agencies reported on their active participation in the workshops organised in 2019 under the Italian chairmanship73 of the ECGFF. These workshops sought to increase awareness and exchange best practices and existing tools on risk management.' (European Commission, 'Joint Staff Working Document. Report on the implementation of the revised EU Maritime Security Strategy Action Pla,. SWD (2020) 252', 23 October 2020).
[148] U. Von der Leyen, 'A Union that Strives for more. My agenda for Europe', *European Commission*, 2019, p.13.
[149] European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013)', 7 February 2013, p.5.
[150] ENISA, 'NIS Directive', n.d..

provide the EU Agency for Network and Information Security (ENISA) with a permanent mandate and plans to introduce a European system for cybersecurity certification to improve the security of networked devices and digital products and services.[151]

The EU launched a new cybersecurity strategy in December 2020.[152] It aims at strengthening Europe's cyber resilience and technological sovereignty. The document lists several initiatives that will link cybersecurity more closely with the EU's new rules on data, algorithms, markets, and Internet services. It came along with a proposal to update the NIS directive[153] and a proposal for the 'Directive on the resilience of critical entities'.[154]

Neither the past nor the current cyber security strategy refers directly to the protection of undersea cable infrastructure. Interviews indicate, however, that strategy makers are well aware of the issue and the cable infrastructure features in the proposal to revise the NIS directive as discussed below.

7.2.1 The European Union Agency for Cybersecurity

ENISA is the European Union Agency for Cybersecurity. ENISA was established in 2004 and gained permanent status with the adoption of the EU Cybersecurity Act.[155] ENISA is involved in a broad range of EU cybersecurity initiatives, including policy development and implementation, certification and standardization for ICT products, services and processes, and capacity building and awareness-raising.

Interviews indicate a high level of awareness at ENISA that cybersecurity is a core factor in subsea data cable protection. However, it was pointed out that cable protection and surveillance is not explicitly an element in EU cybersecurity policies. Yet, the issue has been discussed, and ENISA plans to publish a study involving the security of subsea data cables in 2022.[156]

As part of the EU's telecom regulatory framework, ENISA has been constructing annual reports on telecom security incidents for the past decade. The annual report provides anonymised and aggregated information about major telecom security incidents based on a national security incident notification scheme for telecom providers.[157] However, damage to submarine data cables does not figure in the reporting so far.

7.2.2 Existing and planned regulation

The protection of undersea cables is dependent on the regulatory regimes in member states. With the transposition of the 'European Electronic Communications Code',[158] telecom providers are obliged to report incidents that had a significant impact on the operation of networks or services to their competent national authorities. While this can include incident reporting on subsea data cables, the implementation

[151] European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM (2017), 477', 18 May 2018.
[152] European Commission, 'Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade', 16 December 2020.
[153] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 2020/0359 (COD)', 16 December 2020.
[154] European Commission, 'Proposal for a Directive of the European Parliament and the of the Council on the resilience of critical entities, 14262/20 + ADD1, 2020/0365 (COD)', 2021.
[155] European Parliament, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)', 7 June 2019.
[156] In 2014, ENISA conducted a study titled 'Protection of Underground Electronic Communications Infrastructure'. It analysed existing initiatives on infrastructure protection deployed by selected Member States.
[157] Latest report: ENISA, 'Telecom Security Incidents 2020 - Annual Report', 26 July 2020.
[158] European Parliament, 'Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code', 17 December 2018.

of the regulation, the ownership and operating structures of the subsea data cable infrastructure, their cross-border and their partially non-national location make the current subsea data cable incident reporting ambiguous.

In the proposal for a revised NIS directive[159], the cable network is explicitly referred to. It states that 'the internal market is more reliant on the functioning of the internet than ever before. The services of virtually all essential and important entities are dependent on services provided over the internet. In order to ensure the smooth provision of services provided by essential and important entities, it is important that public electronic communications networks, such as, for example, internet backbones or submarine communications cables, have appropriate cybersecurity measures in place and report incidents in relation thereto.' It is, however, too early to say if and how the updated NIS directive will include regulation on subsea data cable protection.[160]

Alongside the proposal for the updated NIS directive, the Commission proposed a directive on the 'Resilience of Critical Entities'.[161] The objective of the directive is to improve the resilience of critical entities against physical threats in a large number of sectors. The proposal thereby aims to expand both the scope and depth of the current 2008 directive, including the coverage of ten sectors: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration and space. The directive aims to establish synergies with the updated NIS directive. If and how this will affect the protection of subsea data cables is uncertain at the time of writing.

7.3 The broader policy context

While maritime security and cyber security are the most immediate policy fields in which subsea data cable resilience matters, a broader policy context is informative both in terms of the issues linked to it and identifying opportunities for better protection on an EU level. We discuss ocean governance and digital policy and infrastructure.

7.3.1 Ocean governance and marine policy

Cables are also an issue within the EU's broader ocean governance and marine policy, given they are at sea. The EU's Integrated Maritime Policy of 2007, supported by its 2012 Blue Growth strategy, emphasizes the importance of marine spatial planning and marine surveillance with a global outlook. The Joint Communication of 10 November 2016 on 'International Ocean Governance: an agenda for the future of our oceans' identifies different maritime crimes as a major challenge and lays out the global maritime ambitions of the EU. It also stresses the need for integrating different policies and engaging in international cooperation and capacity building. While none of these policies explicitly mentions cables, they provide an important framework for the EU's maritime agencies and devise ocean governance tools that are prospectively useful in cable protection.

This includes, in particular, the emphasis on maritime surveillance but also the toolbox of marine spatial planning. Under ocean governance policies, one of the declared goals is to expand marine protected areas. Given that marine activities are very restricted in marine protected areas, they are spaces in which cables would face fewer risks. Since cable installations have a very limited environmental impact once on the ground, there is a strong synergy between the objectives of marine protection and data cable resilience. Indeed, analysts have highlighted that cable corridors within marine protected areas are a potential

[159] European Parliament, 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', 19 July 2016.
[160] Trilogue interinstitutional negotiations started on 13 January 2022.
[161] European Commission, 'Proposal for a Directive of the European Parliament and the of the Council on the resilience of critical entities, 14262/20 + ADD1, 2020/0365 (COD)', 2021.

solution to enhance cable resilience.[162] Hence, there are potential synergies between marine protection and cable resilience, and the European Environmental Agency could have a prospective role in this regard.

7.3.2 Digital policy and infrastructure

The inexorable and omnipresent digital development inserts technologies of foreign companies and states directly into the everyday life of European citizens and the everyday operations of European critical infrastructures. In response, the EU has come to view external influence and dependencies as a potential security threat and is seeking to reclaim control over key critical technologies and infrastructures. This has led to calls for achieving European digital sovereignty based on retaining and retaking control of data, technologies, and infrastructures. The European Commission has released a draft of new digital policy initiatives, including strategies on AI, data, the digital future, European industry, and the proposed 'Digital Markets Act', 'Digital Services Act' and the European Data Gateway Platforms Strategy.

The submarine data cable network is a significant element in achieving European digital sovereignty. However, subsea data cables have not yet received attention from EU policy and discourse on digital sovereignty. Relatedly, no evaluation or assessment seems to have been made of the EU's dependence on foreign infrastructure and technology in this area.

7.4 External action

External action both in terms of the Common Security and Defence Policy (CSDP) as well as the European Development Policy is directly relevant for cable resilience given the transnational structure of the network with a focus on nodal points and the countries that the EU is connected to, but also the potential impact of cable failure on peace and security in the Global South.

Neither the 2017 European Consensus on Development nor the 2016 EU's Global Strategy directly refers to subsea data cables, albeit highlighting the importance of critical infrastructure. The 2020 European Union Security Union Strategy and the 2022 Strategic Compass strongly emphasise digital infrastructure protection, both in physical and cyber terms. Surprisingly they do not include a detailed action on subsea data cables.[163] However, the documents indicate awareness of the issue. Below, we provide a more detailed review of a range of strategies and activities that provide opportunities to embed cable resilience in external action.

7.4.1 Development partnerships

In its introduction to international development partnerships under the resilience, peace and security theme, the Commission at least hints at the topic when it stresses the objective to 'mitigate global and emerging threats, such as terrorism and violent extremism, transnational organised crime (including environmental crime, illicit trafficking and cybercrime), protection and resilience of critical infrastructure (including public, maritime, air and cyberspaces) - as multipliers of global security challenges'.[164]

Under the theme of Digital Partnerships,[165] the Commission, in particular, works with the African continent to enhance digital infrastructure, which includes the development of cable networks (e.g. under the Africa

[162] L. Carter, D. Burnett, S. Drew, G. Marle, L. Hagadorn, D. Bartlett-McNeil, and N. Irvine, 'Submarine Cables and the Oceans – Connecting the World', *UNEP-WCMC Biodiversity Series,* No. 31, 2009.
[163] European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM (2020) 605', 24 July 2020; European External Action Service, 'A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security', 2020.
[164] European Commission, 'Resilience, peace and security', n.d..
[165] European Commission, 'Global digital partnerships', n.d..

Connect project[166]). Many countries in North Africa are nodal states for European cable connection, but no specific development policy actions concerning the nodal or connecting states could be identified.

7.4.2 Foreign policy instruments

Initiated under the Instrument contributing to Stability and Peace (IcSP) and currently funded through the Neighbourhood, Development and International Cooperation Instrument (NDICI), the EU runs the Critical Maritime Routes (CMR) programme. The programme is one of the most important global capacity-building providers in maritime security and ocean governance operating in regions such as the Gulf of Guinea and the Western Indian Ocean. While mainly foregrounding piracy and maritime crime challenges, the CMR projects work towards institution building and improving maritime law enforcement more generally. Subsea cable resilience is not yet an explicit topic in the programme. Yet, there are joint discussions with the UN Office on Drugs and Crime's (UNODC) Global Maritime Crime Programme that have addressed the cable resilience of small states in the Western Indian Ocean region.[167]

7.4.3 EU Diplomacy and EEAS

Diplomacy is notably important concerning the two nodal states, Egypt and Marocco, but also concerning the vast range of connected states in the North Atlantic (U.S., Canada, Norway), South Atlantic (Brazil, West Africa), the Mediterranean region (e.g. Tunesia, Israel), as well as the Indo-Pacific region. No immediate diplomatic actions concerning the nodal or connecting states could be identified that are currently carried out by the European External Action Service (EEAS). Regional strategies, however, emphasise connectivity and infrastructures as key dimensions. For instance, the EU strategy for cooperation in the Indo-Pacific emphasises the importance of infrastructure and digital partnerships but does not assign an immediate action to subsea cables.[168] However, interviews indicate basic awareness of the issue of cable resilience.

7.4.4 Military coordination, EDA and PESCO

In the area of military and defence coordination, the EU Military Committee has discussed the issue of subsea data cables within its debates on maritime security. For instance, under the 2021 Portuguese presidency, events on maritime security included the discussion of subsea data cables.[169] The major new initiative for defence planning, the Strategic Compass, has a significant maritime component and its focus on resilience includes attention to critical maritime infrastructure.[170] However, there is no direct mention of undersea cables in the final version of the Strategic Compass.

Within the frame of the EDA, the Maritime Surveillance project (MARSUR), running since 2006, continues to develop a recognised maritime picture for European navies and provides the means for military information exchange on the basis of its MARSUR Exchange System.[171] The system is intended to provide a military layer to CISE and could play an important role in particular concerning the surveillance of cables and suspicious activity on the high seas. Other relevant EDA projects are in the frame of the 'European Unmanned Maritime Systems for Mine Counter Measures and other Naval applications', the 'Unmanned

[166] European Commission, 'AfricaConnect', 20 December 2019.
[167] Ref to UNODC, 'Key actions to protect submarine cables from criminal activity identified at UNODC global expert meeting', 7 February 2019.
[168] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. The EU strategy for cooperation in the Indo-Pacific, JOIN (2021) 24', *European Commission*, 16 September 2019.
[169] Government of Portugal, 'Documentation of Seminar on Maritime Security. EUMC Mini Away Day', 2 June 2021.
[170] D. Fiott, 'Naval Gazing? The Strategic Compass and the EU's Maritime Presence', *European Union Institute for Security Studies*, July 2021, p. 36; European External Action Service, 'A Strategic Compass for Security and Defence for a European Union that protects its citizens, values and interests and contributes to international peace and security', 2020, p. 36.
[171] European Defence Agency, 'Maritime Surveillance (MARSUR)', n.d..

Maritime Systems', the 'Maritime Mine Counter Measures' programme areas. Also, the EDA led CapTech Maritime provides a relevant forum for the discussion on developing relevant defence systems.

In so far as they improve surveillance, and in particular sub-sea capabilities, a number of projects in the Permanent Structured Cooperation (PESCO) and the EDA have relevance for cable resilience. Projects such as 'Maritime Unmanned Anti-Submarine System (MUSAS)'[172] 'Harbour & Maritime Surveillance and Protection (HARMSPRO)'[173] and 'Maritime (semi-) Autonomous Systems for Mine Countermeasures (MAS MCM)'[174] are important as these aim at improving command and control capabilities, developing new integrative platforms of multiple assets and sensors that can assist in countering threats to the cable network, as well as new mine-hunting capabilities.

7.4.5 Response to hybrid threats

The 2016 joint framework on countering hybrid threats provides another important instrument for cable resilience.[175] It established the Hybrid Fusion Cellat the level of EU institutions as part of the EU Intelligence and Situation Centre (INTCEN), which provides an important analytical capability for developing scenarios and enhancing information exchange on hybrid threats. The work has included maritime and transport security issues. It is an important instrument in the EU-NATO cooperation, in particular, to facilitate joint planning and exercises. The European Centre of Excellence for Countering Hybrid Threats based in Helsinki is another tool in this collaboration. The Centre provides analysis and guidance documents and serves as a platform for discussing challenges. In 2018 it launched a Network on Maritime Vulnerabilities and Resilience with three workstreams: Ports, Shipping and Underwater Cables.[176] The network aims at integrating industry representatives. The Centre so far has not held a dedicated follow-up event. In its working paper series, cable failure is listed as one among other scenarios of hybrid threats in the maritime domain.[177]

7.4.6 EU-NATO partnership

The political attention to hybrid threats also provides the main collaboration link between the EU and NATO. Contrary to the EU, NATO leadership has recurrently alerted to threats to the cable infrastructure in public speeches, with a primary focus on Russian naval activities.[178]

In October 2020, NATO defence ministers discussed an assessment of Russian threats to the security of undersea cables.[179] NATO General Secretary Jens Stoltenberg declared that threats to undersea infrastructures are taken very seriously and are closely monitored. The Communique of the 2021 Brussels Summit includes an explicit commitment to the issue and argues that NATO members 'will maintain awareness of any potential threats to our critical undersea infrastructure and will continue to address them nationally and, where needed, collectively.'[180]

[172] Permanent Structured Cooperation, 'Maritime Unmanned Anti-Submarine System (MUSAS)', European Union, n.d..
[173] Permanent Structured Cooperation, 'Harbour and Maritime Surveillance and Protection (HARMSPRO)', European Union, n.d..
[174] Permanent Structured Cooperation, 'Maritime (Semi-) Autonomous Systems for Mine Countermeasures (MAS MCM)', European Union, n.d..
[175] European Commission: 'Joint Communication to the European Parliament and the Council on a Joint Framework on countering hybrid threats - a European Union response', JOIN(2016) 18 final, 6. April 2016.
[176] Hybrid CoE, 'Network on Maritime vulnerabilities and resilience launched', 16 March 2018.
[177] T. Lohela, and V. Schatz, 'Hybrid CoE Working Paper 5: HANDBOOK ON MARITIME HYBRID THREATS — 10 Scenarios and Legal Scans', *Hybrid CoE*, 22 November 2019.
[178] P. Morcos, and C. Wall, 'Invisible and Vital: Undersea Cables and Transatlantic Security', *Center for Strategic and International Studies*, 11 June 2021; A. Brzozowski, 'NATO seeks ways of protecting undersea cables from Russian attacks', *Euractiv*, 23 October 2020.
[179] A. Brzozowski, 'NATO seeks ways of protecting undersea cables from Russian attacks', *Euractiv*, 23 October 2020.
[180] NATO, 'Brussels Summit Communiqué', 14 June 2021.

As the most immediate measure, NATO reactivated the new North Atlantic Command - Joint Force Command Norfolk, based in Norfolk, USA, which opened in September 2020. The Command, established to protect sea lanes between Europe and North America, has been the first NATO headquarters dedicated to the Atlantic since 2003. According to NATO sources, 'one of the tasks of this new North Atlantic Command is also to look into how to protect, how to monitor threats against undersea infrastructure.'[181] The Command was declared fully operational in July 2021.[182] NATO's precise activities, exercises and defence planning concerning the issues are classified and not in the public domain.

NATO operates four Centres of Excellence with a maritime focus.[183] These centres provide analysis and engagement opportunities through workshops and conferences. Of the centres, the NATO Maritime Security Centre of Excellence, based in Turkey, has the most explicitly started to address infrastructures and launched a series of workshops on the theme in 2021, with the first one scheduled in March 2022. None of the centres has so far, however, published assessments or guidance documents.

7.4.7 Brexit

The collaboration with NATO is gaining importance, not the least in the light of the United Kingdom's decision to leave the EU. Section 3.2 indicates that the UK is a key connecting state for the EU's data transmission to North America. While Denmark as a strategic site is gaining importance, the UK will remain one of the most important nodal points in North Atlantic connectivity.

The relations between the UK and the EU continue to be in flux, and no precise new regulatory framework that would deal with subsea infrastructure or data connectivity is available so far. Maritime matters have proven controversial as controversies over fisheries and irregular migration highlight, yet cable security is a common interest.

British security leadership has recurrently flagged cable protection as a top priority security issue. For instance, in January 2022, the Chief of Defense Staff warned that Russian submarine activity is threatening underwater cables.[184] He added that any damage to cables would be considered an act of war.[185] A series of documents indicate the UK's high-level attention to the issue. This includes the 2021 UK's Integrated Review of Security, Defense, Development and Foreign Policy, a 2022 report of the British Parliament on the UN Convention on the Law of the Sea[186], as well as the forthcoming refreshed National Maritime Security Strategy, which is expected to include an entire section on the issue.[187]

As the most immediate measure, the UK has announced the acquisition of a new vessel. The Multi Role Ocean Surveillance ship (MROSS) will be explicitly tasked with the surveillance of undersea infrastructure to detect operations in the vicinity of cable locations. The ship will be equipped with unmanned underwater drones and is expected to be in service in 2024.[188]

[181] NATO, 'Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers', 22 October 2020.
[182] NATO, 'Allied Joint Force Command Norfolk declares Full Operational Capability', 15 July 2021.
[183] NATO Maritime Security Centre of Excellence, the NATO Centre of Excellence of Combined Joint Operations from the Sea, NATO Centre of Excellence for Naval Mine Warfare, and NATO Centre of Excellence for Operations in Confined and Shallow Waters. In addition, it also operates the NATO Maritime Interdiction Operational Training Center and the NATO Centre for Maritime Research and Experimentation.
[184] Guardian (The), 'UK military chief warns of Russian threat to vital undersea cables', 8 January 2022.
[185] D. Kundaliya, 'Russian harm to underwater cables could be 'act of war', UK defence chief warns', *computing*, 10 January 2022.
[186] International Relations and Defence Committee, 'UNCLOS: fit for purpose in the 21st century?', *United Kingdom House of Lords*, 2021.
[187] C. Bueger, and T. Edmunds, 'Innovation and New Strategic Choices. Refreshing the UK's National Strategy for Maritime Security', *The RUSI Journal, 166*(4), pp. 66-75.
[188] GlobalSecurity.org, 'Multi Role Ocean Surveillance ship (MROSS)', n.d..

7.5 Synthesis

Our review of EU-level awareness and initiatives shows that cable resilience is a truly cross-cutting issue. While maritime security and cyber security are the policy domains most directly relevant, they are not only complex issue domains in their own right, but also other EU institutions and domains matter for cable resilience. This includes ocean governance, digital sovereignty, critical infrastructure policy, and various aspects of external action, from defence policy, diplomacy, and development to the relations between NATO and the UK. On the one side, this complexity is problematic as it risks that none of the domains and the actors dominating them will take full authority to deal with the issue. The opposite scenario is thinkable too, where it might lead to a situation where multiple agencies compete for overtaking the coordination function and other resources. This could produce a situation of duplication and overlap. Critical will be how to overcome the civil-military divide, in so far as cable resilience is both a civil and safety issue, as much as a military one. It concerns internal security and sovereign territories (territorial waters) as well as external security (high seas). However, the growing awareness of the issue indicates that ample opportunities exist for improving resilience within existing structures and agencies. This is the issue we turn towards next.

8 Recommendations

Several recommendations follow from our analysis. These can be broadly clustered around the need to further enhance EU-wide awareness and understanding, improve coordination and information sharing, advance surveillance capabilities, strengthen response mechanisms, and mainstream the topic across external action.

8.1 Awareness and prioritization

Our review indicates that there is a basic level of attention across Member States and EU institutions. Much of this attention so far is basic and at the rhetorical level, with only sparse immediate actions linked to cable protection. There is also an indication that there continues to be a lack of knowledge of how the cable system operates, its legal status, and its key vulnerabilities. As an immediate step, the European Parliament could ensure that data cable protection is adequately considered in a number of currently ongoing strategy and review processes.

8.1.1 Refreshed EU Maritime Security Strategy

The European Parliament could make efforts to ensure that cable protection is adequately and prominently considered in the EU's planned revision of the Maritime Security Strategy and its future Action Plans. In the 2014 EUMSS, it is only vaguely included in the core strategic interests, and no direct action is devoted to implementation. The European Parliament could encourage the institutions leading the drafting process (EEAS, DG MARE) to prioritize data cable protection and encourage them to conduct substantial consultations with the relevant technical agencies (EFCA, EMSA, ENISA, Frontex) concerning potential actions.

8.1.2 Review of EMSA mandate

The mandate of EMSA is currently under review by DG MOVE. The European Parliament could invite DG MOVE and EMSA to consider if and how subsea cables could form part of the revised mandate (see 8.3: Surveillance).

8.1.3 Review of the links between EU digital policies and subsea cables

The European Parliament could – together with the Commission and the Member States – consider reviewing how subsea cables relate to the ambition of EU technological sovereignty. This includes examining the role of undersea cables in relation to existing digital policy initiatives such as Europe's Digital Decade, The European Strategy for Data, GAIA X, the Digital Markets Act and the Digital Services Act.

8.1.4 Coastguard training

The European Parliament could encourage Frontex, EFCA and EMSA to ensure that joint training and educational programmes include a module on the particularities of subsea data cable, their legal status, regulatory challenges and relations to the industry. This will enhance long term awareness and understanding by coastguard function agencies.

8.1.5 Awareness-raising events

The European Parliament could encourage different bodies of the EU or affiliated with it to organise events that raise the level of awareness and knowledge on the topic. Entities such as the European Coast Guard Functions Forum, the European Centre of Excellence for Countering Hybrid Threats or the EU Military Committee should be invited to hold a dedicated event on the issue and produce public documentation of the discussions.

8.1.6 National risk assessments

The European Parliament could encourage EU Member States to conduct their own survey of cables and landing stations, assess their vulnerabilities and risks, available repair and response mechanisms, and relation to the industry, and share the results with all Member States and EU bodies.

8.2 Information sharing

A key hindrance to effective governance and protection of the cable network is the lack of systematic data on regulatory agencies, regulatory regimes concerning the laying and repair of cables, current protection measures, national surveillance capabilities and operations, cable ownership, and damage incidents as well as suspicious activity.

8.2.1 Establish basic information sharing and coordination mechanism

Improving information sharing could be initially handled by a cross-EU working group that includes the cable industry. The European Parliament could ask the commission to organise a Subsea Cable Resilience Coordination working group. The working group should include the different DGs, EEAS, as well as the relevant technical agencies (EFCA, EMSA, Frontex, ENISA, EEAS). The working group could discuss and review on a strategic level how responses could be better harmonised. Member States should be encouraged to share their risk assessments and best practices in such a group.

8.2.2 Law enforcement coordination

On a Member State level, the ECGFF could be invited to establish a working group to discuss the role of law enforcement agencies in ensuring cable protection and in developing shared standard operating procedures. The successful work that the ECGFF carried out in maritime cyber security for ports and shipping indicates that the forum could be a major format to address the issue.

8.2.3 Reporting of faults and breakdowns

No voluntary or compulsory reporting mechanism of cable faults exists on EU level or within the EU Member States. The UK, for instance, has a voluntary reporting mechanism, while the US has a compulsory one. A reporting mechanism is key to identifying patterns and trends, conducting appropriate risk analyses, and reviewing repair infrastructure's sufficiency.

The EP could call upon the Commission to identify mechanisms for reporting and recording cable fault data, for instance, by mandating one of the technical agencies to collect such data (e.g. ENISA, EMSA). A better implementation of the 'European Electronic Communications Code' and the revised NIS directive provides important opportunities in this regard.

Since cable faults that can impact EU connectivity may occur in the jurisdictions of non-EU member states, in particular the United Kingdom, Egypt and other states in the MENA region, West Africa or South America, a reporting mechanism should ideally go beyond EU Member States. The EU could ask the EEAS with considering if and how frameworks can be developed on a bilateral or regional level (e.g. for the Mediterranean, South Atlantic).

8.3 Surveillance

A key aspect of cable protection is appropriate surveillance and identification of suspicious activities. Cable surveillance is currently mainly provided by the industry. The industry monitors its cables in order to locate any cable breaks rapidly. It also draws on the Automatic Identification System (AIS) data as evidence in civil law cases.

A number of states conduct surveillance with regards to high risk or suspicious activities in the vicinity of cable laying areas as part of their overall maritime domain awareness programmes or fishery control activities. These mainly focus on territorial waters and Exclusive Economic Zones.

This implies that currently, no surveillance data concerning repeat offenders or suspicious activities exist across the EU.

8.3.1 Integrate cable surveillance in the Common Information Sharing Environment (CISE)

The EU has the required capabilities to conduct surveillance and risk analysis as it concerns the surface and suspicious non-military activities. The maritime satellite pictures and ship positioning data by EMSA and EFCA can be used for such purposes. Suspicious behaviour can be monitored through dedicated anomalous behaviour algorithms supported by analysts. CISE combined with the resources of MIC-RAN and MARSUR can be used to share the analysis across the EU and the EU Member States.

8.3.2 Invite position paper from EMSA and Frontex concerning feasibility

Employing such existing capabilities requires a revised mandate for EMSA and Frontex and dedicated resources. The EMSA mandate is currently under review by the Commission, which provides the opportunity to include the surveillance of cables in the spectrum of tasks. The EP could invite EMSA to provide a review on feasibility and ask the Commission to include the task in its mandate revision process. The European Parliament could also invite a statement from FRONTEX concerning the technical possibilities of integrating the task in CISE, EUROSUR and MIC-RAN.

8.3.3 Integrating surveillance data from industry

The European Parliament should request that a new Cable Resilience Coordination Working Group (see 8.2.1) develops a proposal on how the surveillance data by the shipping industry and cable industry can be integrated into the risk analyses and the relations to the maritime industry can be improved.

8.3.4 Subsea surveillance capabilities

The European Parliament could ask the HRVP to task the EDA to conduct a survey of current subsea surveillance technology that can be used to monitor activities in cable locations and whether and how Member States use these capabilities. The European Parliament could invite EDA to provide a position on if and how relevant information on subsea behaviour is or could be integrated into MARSUR. The European Parliament should also invite EDA to task their consortia that develop MUSAS, HARMSPRO and MAS MCM to provide an analysis of what role the new technology can play in the underwater surveillance of cables. The European Parliament could encourage the Member States via the Permanent Structured Cooperation (PESCO) and the EU Military Committee (EUMC) to consider which new defence projects could make a contribution to undersea surveillance.

8.4 Repair capabilities and regulations

A key and often neglected vulnerability of the cable infrastructure is the capabilities and regulations for repair. The capabilities within Europe are very limited, and the legal regulations of repair activities are not harmonized across Europe. The repair infrastructure is often not featured in risk analyses, although it is in larger-scale coordinated attack scenarios.

8.4.1 EU harmonization of regulations

The European Parliament could encourage the Commission to initiate a legal review and harmonization process for cable repair ships and activities. At the minimum, the Commission could issue a best practice guidance in particular for vulnerable Member States and regions.

8.4.2 Review of Member State dependencies

The European Parliament could invite EU Member States to review their reliance on repair infrastructure, their legal regulation, and the awareness within their respective agencies concerning the international law regulating cables to identify the potential for minimizing delays in repair.

8.4.3 EU repair capabilities

The European Parliament could invite EDA and PESCO to consider if and how the EU could develop or contract a standing repair facility and ship, which would provide a contingency for the scenario of a larger attack.

8.5 Cable corridors and marine protected areas

The most effective way of protecting cables is through cable corridors that are closely monitored. There is a high potential for synergies with ocean policies and marine environmental protection. Planned cable installations could be well integrated into marine protected areas and no-fishing zones. This requires a consideration of the plans and activities of the cable industry in marine spatial planning processes.

The European Parliament could invite DG MARE, EEA and other maritime regulators to comment on and suggest ways how cable protection can be integrated into marine spatial planning and other environmental protection initiatives.

8.6 EU – NATO collaboration and Brexit

The North Atlantic region and British territorial waters are vital to the EU's connectivity. Both NATO and the UK have given the protection of cables a high strategic priority. The United States and the UK's capabilities will be essential in monitoring cables in the North Atlantic, North Sea, as well as the Mediterranean. Given that the majority of EU military capabilities available for protection and surveillance on the high seas are shared between the operational tasks of the EU and NATO, the EU needs to strengthen cooperation in the response wherever possible.

Concrete measures could be in information sharing concerning breakdowns and suspicious behaviour. Any planned events and coordination formats would benefit from integrating NATO member states and entities, particularly the UK, as much as possible. This could, for example, be through coordinated awareness activities with NATO's Centres of Excellence (e.g. the Maritime Security Centre of Excellence based in Turkey), and the establishment of dedicated coordination facilities, taking informal task-specific entities such as the Maritime Analysis and Operations Centre Narcotics[189] as a role model. This would also ensure that any tensions regarding the marine activities of Turkey in the Mediterranean will not have an effect on subsea data cable security.

8.7 Other external action

International collaboration and capacity building are vital in ensuring the EU's connectivity and enabling less developed countries to advance their digital economies and benefit from new forms of growth.

8.7.1 Mainstreaming cable resilience

The European Parliament could ensure that cable resilience is closely integrated and mainstreamed across EEAS and INTPA programmes and activities. The EP could invite the EEAS to consider cable resilience as a core feature in any planned regional strategies.

[189] Maritime Operations and Analysis Centre, 'Narcotics', n.d..

8.7.2 Capacity-building work

The European Parliament could encourage the EEAS to ensure that cable resilience forms part of ongoing and planned maritime security and cyber policy capacity building projects with a particular view on vulnerable states, such as small island developing states that are heavily dependent on single cable connections. Partnerships with international organizations active in the area, such as the UNODC's Global Maritime Crime Programme, could be very valuable.

8.7.3 International legal efforts

The European Parliament could further invite the EEAS to elaborate on whether and how opportunities exist to develop regional agreements or an international treaty that provide legal certainty on the rules and responsibilities of states in international waters. EEAS would need to consult closely with the International Cable Protection Committee and legal experts in this regard.

8.8 Cable ownership and industry cooperation

Undersea cables are owned and operated by combinations of private companies, state-owned firms, and international consortia from around the world. This study shows that submarine data cables are a major vector of influence for companies and states on the global internet, including its functioning, development, and security. Overview of cable ownership and strong collaboration with the industry is hence vital.

8.8.1 Review of cable ownership and risk assessment for future cable projects

The European Parliament could invite EU Member States to review ownership of existing and planned cables in order to identify potential risks of a single company/country's dependencies. Relatedly, the EP could promote integrating future cable projects into the national risk assessments (see 8.1).

8.8.2 Strengthening cooperation

The European Parliament could ask the new Coordination Working Group (see 8.2.1) to develop a proposal for how cable protection can be strengthened through improved industry cooperation (between cable owners, tele network operators etc.) and cooperation between the industry, the member states, and the EU. The proposal should consider the establishment of an industry-specific, pan-European public-private Information Sharing and Analysis Centre (ISAC).

8.9 Future inquiries

Several strategic gaps exist in the current knowledge of cable resilience in Europe, and substantial analyses are required to fill these.

8.9.1 Military infrastructures

Military infrastructures and operations are heavily dependent on reliable cable connectivity. With the rise of integrated warfare capabilities, this dependency is growing. The European Parliament should commission a dedicated vulnerability assessment for military infrastructures and capabilities and how cable failure might infringe on operations. A particular focus should be given to overseas naval bases as well as forward employment operations. Such an assessment would have to draw on classified information.

8.9.2 Space-based redundancy

Space-based internet provision is a growing market, and technology is continuously advanced. While these will not replace cables in the mid to long term future, given lower bandwidth, reliability issues and weather dependency, their role in providing civil and military resilience in attack scenarios requires further elaboration.

8.9.3 Other subsea cable infrastructure

Data cables are not the only subsea infrastructure that requires protection. Increasingly, undersea electricity cables are important in the European energy markets. As part of the green revolution, dependency on transnational undersea electricity cable connections and connections to offshore wind farms will increase. For instance, several installations in the Mediterranean area are in the planning stage, which connect North Africa and Italy and transport both data and electricity. The European Parliament should consider commissioning assessments concerning the impact of subsea cables on future energy security and if and how electricity cables are best protected by the same means.

8.9.4 Contingency planning

The current study implies that the EU and its Member States so far lack EU contingency planning and crisis management measures in case of a major breakdown scenario. The European Parliament could propose to the other EU institutions to draw on table top exercises and expert analysis to develop a dedicated contingency plan that operates across the EU and provides best practices for the Member States.

Annex I - Bibliography

Aceto, G., Botta, A., Marchetta, P., Persico, V., and Pescapé, A., 'A Comprehensive Survey on Internet Outages', *Journal of Network and Computer Applications*, Issue 113, March 2019, pp, 36–63, retrieved from: https://doi.org/10.1016/j.jnca.2018.03.026

ACMA, 'Atlantic Cable Maintenance & Repair Agreement', n.d., retrieved from: https://www.acma2017.com

Agarwala, N., '"Green cables" – Development, opportunities and legal challenges: Part I', *Maritime Affairs: Journal of the National Maritime Foundation of India*, 2018, *14*(2), pp. 49–62, retrieved from: https://doi.org/10.1080/09733159.2018.1562456

Agarwala, N., 'Green cables – Development, opportunities and legal challenges; Part-II', *Maritime Affairs: Journal of the National Maritime Foundation of India*, *15*(1), 2019, pp. 93–107, retrieved from: https://doi.org/10.1080/09733159.2019.1631538

Agrawal, G. P., 'Optical Communication: Its History and Recent Progress', *In Optics in Our Time*, 2016, pp. 177–199, retrieved from: https://doi.org/10.1007/978-3-319-31903-2_8

Ankel, S., 'Russian intelligence agents reportedly went to Ireland to inspect undersea cables, and it's reigniting fears they could cut them and take entire countries offline', *Business Insider*, 17 February 2020, retrieved from: https://www.businessinsider.com/russian-agents-went-to-ireland-to-inspect-undersea-cables-report-2020-2?r=US&IR=T

Ardemagni, E., 'Red Sea Security: How Yemen Tests The "Abraham Equation"', *Italian Institute for International Political Studies*, 15 December 2021, retrieved from: https://www.ispionline.it/en/pubblicazione/red-sea-security-how-yemen-tests-abraham-equation-32650

Article 51(5)(b), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, retrieved from: https://ihl-databases.icrc.org/ihl/WebART/470-750065

Baumann, J., 'Publisher of subsea cable news uses ArcGIS for industry analysis and interactive mapping', *Submarine Telecoms Magazine*, Issue 116, 2021, pp. 36–37

BBC, 'Portugal navy escorts Russian ship away from coast', 5 November 2014, retrieved from: https://www.bbc.com/news/world-europe-29919036

Beckman, R., 'Submarine Cables – A Critically Important but Neglected Area of the Law of the Sea', *ISIL Conference*, 2010, pp. 12-16, retrieved from: https://cil.nus.edu.sg/wp-content/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables-rev-8-Jan-10.pdf

Bergin, A., and Bashfield, S., 'Digital age lies vulnerable to threats from underwater', *Australian Strategic Policy Institute*, 18 October 2021, retrieved from https://www.aspi.org.au/opinion/digital-age-lies-vulnerable-threats-underwater

Besanger, S., 'La Russie peut-elle vraiment priver l'Europe d'internet en coupant les câbles sous-marins?', *Ouest France*, 9 March 2022, retrieved from: https://www.ouest-france.fr/leditiondusoir/2022-03-09/la-russie-peut-elle-vraiment-priver-l-europe-d-internet-en-coupant-les-cables-sous-marins-eae91619-ecea-4cee-a20e-c223165a9a0b

Birnbaum, M., 'Russian submarines are prowling around vital undersea cables. It's making NATO nervous', *The Washington Post*, 22 December 2017, retrieved from: https://www.washingtonpost.com/

world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?utm_term=.c01da94c979e

Bossler, A. M., and Berenblum, T., 'Introduction: new directions in cybercrime research', *Journal of Crime and Justice*, *42*(5), 2019, pp. 495-499, retrieved from: https://doi.org/10.1080/0735648X.2019.1692426

Breitenbauch, H., and Liebetrau, T., 'Technology Competition, Strategic implications for the West and Denmark', *Djøf Publishing in cooperation with the Centre for Military Studies*, 2021, retrieved from: https://cms.polsci.ku.dk/english/publications/technology-competition-strategic-implications-for-the-west-and-denmark/download-cms-report/CMS_Report_2021__6_-_Technology_Competition__Strategic_Implications_for_the_West_and_DK.pdf

Brzozowski, A., 'NATO seeks ways of protecting undersea cables from Russian attacks', *Euractiv*, 23 October 2020, retrieved from: https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/

Bueger, C., and Edmunds, T., 'Beyond Seablindness: A New Agenda For Maritime Security Studies, International Affairs', *International Affairs*, *93*(6), pp. 1293–1311

Bueger, C., and Edmunds, T., 'Innovation and New Strategic Choices. Refreshing the UK's National Strategy for Maritime Security', *The RUSI Journal, 166*(4), pp. 66-75

Bueger, C., and Liebetrau, T., 'Governing hidden infrastructure: The security politics of the global submarine data cable network', *Contemporary Security Policy*, *42*(3), 2021, pp. 391-413

Bueger, C., and Stockbruegger, J., 'Maritime security and the Western Indian Ocean's militarisation dilemma', *African Security Review*, 2022 doi: 10.1080/10246029.2022.2053556.

Burnett, D. R., Beckman, R., and Davenport, T. M. (Eds.), 'Submarine Cables. The Handbook of Law and Policy', 2013.

Carter, L., Burnett, D., Drew, S., Marle, G., Hagadorn, L., Bartlett-McNeil, D., and Irvine, N., 'Submarine Cables and the Oceans – Connecting the World', *UNEP-WCMC Biodiversity Series,* No. 31, 2009, retrieved from: https://www.iscpc.org/documents/?id=132

Cerulus, L., 'Lisbon eyes undersea cable investment to bolster EU tech infrastructure', *Politico*, 10 December 2020, retrieved from: https://www.politico.eu/article/submarine-cables-europe-lisbon-eyes-undersea-investment-bolster-tech-infrastructure/

Cisco, 'Cisco Annual Internet Report (2018–2023)', 2020, retrieved from https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Coffey, V., 'Sea change: The challenges facing submarine optical communications', *Optics and Photonics News*, 2014, *25*(3), pp. 26–33, retrieved from: https://opg.optica.org/DirectPDFAccess/EAABFF7C-F582-4037-A851B8AA30E3FA59_281128/opn-25-3-26.pdf?da=1&id=281128&seq=0&mobile=no

Commission on the Defence Forces, 'Report of the Commission on the Defence Forces', 2022, retrieved from: https://www.rte.ie/documents/news/2022/02/215358-a21b9438-45a6-4c26-a508-c0d1aeeeb336.pdf

Connolly R., and Boulègue, M., 'Russia's New State Armament Programme, Implications for the Russian Armed Forces and Military Capabilities to 2027', *Chatham House the Royal Institute of International Affairs*,

May 2018, retrieved from: https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf

Council of the European Union, 'Council conclusions on the revision of the European Union Maritime Security Strategy (EUMSS) Action Plan 10494/18', 26 June 2018, retrieved from: https://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf

Council of the European Union, 'European Union Maritime Security Strategy, 11205/14', 24 June 2014, retrieved from: https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf

Courtois, O., Bardelay-Guyot, C., 'Architectures and management of submarine networks', in J. Chesnoy (Ed.), *Undersea Fiber Communication Systems (Second Edition*), 2016, pp. 343-380.

Danish Government, 'Bekendtgørelse af lov om kystbeskyttelse m.v.', 29 May 2020, retrieved from: https://www.retsinformation.dk/eli/lta/2020/705

Danish Government, 'Bekendtgørelse om beskyttelse af søkabler og undersøiske rørledninger', 27 November 1992, retrieved from: https://www.retsinformation.dk/eli/lta/1992/939

Davenport, T., 'Submarine Cables, Cybersecurity: an Intersectional Analysis', *Catholic University Journal of Law and Technology*, *24*(1), 2015, pp. 57-109

Data Center Map ApS, 'Data Center Map', 2022, retrieved from: https://www.datacentermap.com/

ENISA, 'NIS Directive', n.d., retrieved from: https://www.enisa.europa.eu/topics/nis-directive

ENISA, 'Telecom Security Incidents 2020 - Annual Report', 26 July 2020, retrieved from: https://www.enisa.europa.eu/publications/telecom-annual-incident-reporting-2020

European Commission, 'AfricaConnect', 20 December 2019, retrieved from: https://ec.europa.eu/international-partnerships/projects/africaconnect_en

European Commission, 'Coast guard cooperation', n.d., retrieved from: https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/coast-guard-cooperation_en

European Commission, 'Commission Staff Working Document. Review of the Common Information Sharing Environment (CISE) for the maritime domain: 2014 – 2019, SWD (2019), 322', 5 September 2019, retrieved from: https://ec.europa.eu/oceans-and-fisheries/system/files/2021-03/swd-2019-322_en_0.pdf

European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM (2020) 605', 24 July 2020, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN

European Commission, 'Global digital partnerships', n.d., retrieved from: https://ec.europa.eu/international-partnerships/topics/digital-partnerships_en

European Commission, 'Joint Communication: The EU's Cybersecurity Strategy for the Digital Decade', 16 December 2020, retrieved from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the

European Union: An Open, Safe and Secure Cyberspace, JOIN(2013)', 7 February 2013, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

European Commission, 'Joint Staff Working Document. Report on the implementation of the revised EU Maritime Security Strategy Action Plan,. SWD (2020) 252', 23 October 2020, retrieved from: https://ec.europa.eu/oceans-and-fisheries/system/files/2021-03/swd-2020-252_en.pdf

European Commission, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on a Joint Framework on countering hybrid threats a European Union response, JOIN(2016) 18 final, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

European Commission, 'Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 2020/0359 (COD)', 16 December 2020, retrieved from: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF

European Commission, 'Proposal for a Directive of the European Parliament and the of the Council on the resilience of critical entities', 14262/20 + ADD1, 2020/0365 (COD), 2021, retrieved from: https://www.consilium.europa.eu/en/press/press-releases/2021/12/20/strengthening-eu-resilience-council-adopts-negotiating-mandate-on-the-resilience-of-critical-entities/#:~:text=The%20Council%20today%20approved%20a,the%20resilience%20of%20critical%20entities.&text=The%20Council%20negotiating%20mandate%20covers,water%2C%20digital%20infrastructure%20and%20space

European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM (2017), 477', 18 May 2018, retrieved from: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2017)477&lang=en

European Commission, 'Report from the Commission to the European Parliament and the Council on the evaluation of the European Border Surveillance System (EUROSUR), COM (2018), 632', 12 September 2018, retrieved from: https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0632/COM_COM(2018)0632_EN.pdf

European Commission, 'Resilience, peace and security', n.d., retrieved from: https://ec.europa.eu/international-partnerships/topics/resilience-peace-and-security

European Defence Agency, 'Maritime Surveillance (MARSUR)', n.d., retrieved from: https://eda.europa.eu/what-we-do/all-activities/activities-search/maritime-surveillance-(marsur)

European External Action Service, 'A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security', 2020, retrieved from: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

European Parliament, 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', 19 July 2016, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

European Parliament, 'Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code', 17 December 2018, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972
European Parliament, 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)', 7 June 2019, retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Eurostat, 'Statistics Explained: Digital economy and society statistics – Enterprises: Access and use of the internet', *European Commission*, 2021, retrieved from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_%20economy_and_society_statistics-enterprises#Access_and_use_of_the_internet

Eurostat, 'Statistics Explained: Digital economy and society statistics – Household and individuals', *European Commission*, 2021, retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

Fiott, D., 'Naval Gazing? The Strategic Compass and the EU's Maritime Presence', *European Union Institute for Security Studies*, July 2021, retrieved from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_16_2021.pdf

Franken, J., Reinhold, T., Reichert, L., and Reuter, C., 'The Digital Divide in State Vulnerability to Submarine Communications Cable Failure', *International Journal of Critical Infrastructure Protection (IJCIP),* 2022 (forthcoming)

Galea, P., 'Seismic history of the Maltese islands and considerations on seismic risk', *Annals of Geophysics*, *50*(6), 2007, pp. 725-740, retrieved from: https://doi.org/10.4401/ag-3053

Gallagher, C., and Carswell, S., 'Russian naval drill to still take place over vital cables, experts believe', *The Irish Times*, 31 January 2022, retrieved from: https://www.irishtimes.com/news/environment/russian-naval-drill-to-still-take-place-over-vital-cables-experts-believe-1.4789421

García Sánchez, I. J., 'Analysis of the National Strategy for Maritime Security 2013. Prosperity and Welfare beyond the Coastline', *Instituto Español de Estudios Estratégicos*, 10 December 2013, retrieved from: https://www.ieee.es/en/Galerias/fichero/docs_analisis/2013/DIEEEA66-2013_EstrategiaSeguridadMaritimaNacional_IJGS_ENGLISH.pdf

Geny, V., 'La Russie peut-elle priver l'Europe d'Internet en sabotant des câbles sous-marins?', *Marianne*, 5 March 2022, retrieved from: https://www.marianne.net/monde/europe/la-russie-peut-elle-priver-leurope-dinternet-en-sabotant-des-cables-sous-marins

GlobalSecurity.org, 'Multi Role Ocean Surveillance ship (MROSS)', n.d., retrieved from: https://www.globalsecurity.org/military/world/europe/hms-mross.htm

Gohdes, A. R., 'Pulling the plug', *Journal of Peace Research*, *52*(3), 2015, pp. 352–367, retrieved from: https://doi.org/10.1177/0022343314551398

Goldrick, J., 'Grey zone operations and the maritime domain', *The Strategist,* 30 October 2018, retrieved from: https://www.aspistrategist.org.au/grey-zone-operations-and-the-maritime-domain/

Government of Portugal, 'Documentation of Seminar on Maritime Security. EUMC Mini Away Day', 2 June 2021

Guardian (The), 'UK military chief warns of Russian threat to vital undersea cables', 8 January 2022, retrieved from: https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables

Guerrero, J., 'Narcosubmarines. Outlaw Innovation and Maritime Interdiction in the War on Drugs', *Singapore: Palgrave Macmillan*, 2020.

High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council. The EU strategy for cooperation in the Indo-Pacific, JOIN (2021) 24', *European Commission*, 16 September 2019, retrieved from: https://www.eeas.europa.eu/sites/default/files/jointcommunication_2021_24_1_en.pdf

Hinck, G., 'Evaluating the Russian Threat to Undersea Cables', *Lawfare*, 5 March 2018, retrieved from: https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables

Hybrid CoE, 'Network on Maritime vulnerabilities and resilience launched', 16 March 2018, retrieved from: https://www.hybridcoe.fi/news/network-on-maritime-vulnerabilities-and-resilience-launched/

Infrapedia, 'Infrastructure Map', 2022, retrieved from: https://www.infrapedia.com/app

Institute for Economics & Peace, 'Global Terrorism Index 2020: Measuring the Impact of Terrorism', 2020, retrieved from: https://reliefweb.int/sites/reliefweb.int/files/resources/GTI-2020-web-2.pdf

International Committee of the Red Cross, 'Customary IHL Database: Rule 8. Definition of Military Objectives', n.d., retrieved from: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule8

International Committee of the Red Cross, 'International humanitarian law and the challenges of contemporary armed conflicts', *32nd International Conference of the Red Cross and Red Crescent, 32IC/15/11*, 2015, retrieved from: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts

International Relations and Defence Committee, 'UNCLOS: fit for purpose in the 21st century?, *United Kingdom House of Lords*, 2021, retrieved from: https://committees.parliament.uk/work/1557/unclos-fit-for-purpose-in-the-21st-century/publications/

International Relations and Defence Committee, 'UNCLOS: the law of the sea in the 21st century', *United Kingdom House of Lords*, 2022, retrieved from: https://publications.parliament.uk/pa/ld5802/ldselect/ldintrel/159/159.pdf

International Telecommunication Union (ITU), 'Interactive Transmission Map', 2020, retrieved from: https://www.itu.int/itu-d/tnd-map-public/

International Telecommunication Union (ITU), 'Measuring digital development: Facts and Figures 2021', 2021, retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

International Telecommunication Union (ITU), 'Small Island Developing States (SIDS) and ICTs', 2019, retrieved from: https://doi.org/11.1002/pub/813cee7c-en

International Telecommunication Union (ITU), 'World Telecommunication/ICT Indicators Database online 23rd Edition', 2019, retrieved from: https://www.itu.int/pub/D-IND-WTID.OL-2019

Internet Live Stats, 'One Second', 2021, retrieved from https://www.internetlivestats.com/one-second/

Kazantzidou-Firtinidou, D., Kyriakides, N., Votsis, R., and Chrysostomou, C. Z., 'Seismic risk assessment as part of the National Risk Assessment for the Republic of Cyprus: from probabilistic to scenario-based approach', *Natural Hazards*, 2022, retrieved from: https://doi.org/10.1007/s11069-021-05200-y

Khazan, O., 'The Creepy, Long-Standing Practice of Undersea Cable Tapping', *The Atlantic*, 16 July 2013, retrieved from: https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/

Kundaliya, D., 'Russian harm to underwater cables could be 'act of war', UK defence chief warns', *computing*, 10 January 2022, retrieved from: https://www.computing.co.uk/news/4042945/russian-harm-underwater-cables-act-war-uk-defence-chief-warns

Lagneau, L., 'Comment la Marine nationale surveille les câbles sous-marins de communication?', *Zone Militaire*, 11 December 2018, retrieved from: http://www.opex360.com/2018/12/11/comment-la-marine-nationale-surveille-les-cables-sous-marins-de-communication/

Lee, Y., 'China's latest weapon against Taiwan: the sand dredger', *Reuters*, 5 February 2021, retrieved from: https://www.reuters.com/article/us-taiwan-china-security-idUSKBN2A51EJ

Lohela, T., and Schatz, V., 'Hybrid CoE Working Paper 5: HANDBOOK ON MARITIME HYBRID THREATS — 10 Scenarios and Legal Scans', *Hybrid CoE*, 22 November 2019, retrieved from: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-5-handbook-on-maritime-hybrid-threats-10-scenarios-and-legal-scans/

Magazine de la Marine Nationale, Issue 3074, December 2018, retrieved from: https://en.calameo.com/read/000331876a2b79c0cb194

Mahlknecht, G., 'Greg's Cable Map', 2016, retrieved from: https://cablemap.info/_default.aspx

Maritime Operations and Analysis Centre, 'Narcotics', n.d., retrieved from: https://maoc.eu

Matley, H. E., 'Closing the gaps in the regulation of submarine cables: lessons from the Australian experience', *Australian Journal of Maritime & Ocean Affairs*, *11*(3), 2019, pp. 165–184, retrieved from: https://doi.org/10.1080/18366503.2019.1653740

Mauldin, A., 'A Complete List of Content Providers' Submarine Cable Holdings', *TeleGeography*, 2021, retrieved from: https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list

Mauldin, A., 'Cable Breakage: When and How Cables Go Down', *TeleGeography*, 3 May 2017, retrieved from: https://blog.telegeography.com/what-happens-when-submarine-cables-break

Mediterranean Cable Maintenance Agreement (MECMA), n.d., retrieved from: https://www.mecmamc.org/public/

Miller, R., 'Brexit Prep Has Boosted Data Centers, Subsea Cables', *Data Center Frontiers*, 2019, retrieved from: https://datacenterfrontier.com/brexit-prep-has-boosted-data-centers-subsea-cables-but-what-now/

Mooney, J., 'Ireland unable to protect subsea cables from Russian attack', *The Times*, 25 November 2021, retrieved from: https://www.thetimes.co.uk/article/ireland-unable-to-protect-subsea-cables-from-russian-attack-39tk0nprd#:~:text=The%20subsea%20cables%20are%20considered,Europe%20and%20the%20United%20States

Morcos, P., and Wall, C., 'Invisible and Vital: Undersea Cables and Transatlantic Security', *Center for Strategic and International Studies*, 11 June 2021, retrieved from: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Nadimi, F., 'Iran and Israel's Undeclared War at Sea (Part 2): The Potential for Military Escalation', *The Washington Institute for Near East Policy*, 13 April 2021, retrieved from: https://www.washingtoninstitute.org/policy-analysis/iran-and-israels-undeclared-war-sea-part-2-potential-military-escalation

National Bureau of Asian Research, 'Backgrounder from the Maritime Awareness Project: Submarine Cables', n.d., retrieved from: https://www.nbr.org/publication/submarine-cables/

National Oceanic and Atmospheric Administration Ocean Exploration, 'How deep is the ocean?', 2021, retrieved from: https://oceanexplorer.noaa.gov/facts/ocean-depth.html

NATO, 'Allied Joint Force Command Norfolk declares Full Operational Capability', 15 July 2021, retrieved from: https://www.nato.int/cps/en/natohq/news_185870.htm?selectedLocale=en

NATO, 'Brussels Summit Communiqué', 14 June 2021, retrieved from: https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en

NATO Cooperative Cyber Defence Centre of Excellence, 'Strategic importance of, and dependence on, undersea cables', 2019, retrieved from: https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf

NATO, 'Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers', 22 October 2020, retrieved from: https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

Nyboe McGhie, S., 'Efter 15 år i blinde under havoverfladen: Nu skal Danmark igen jagte russiske ubåde', *Berlingske*, 6 December 2019, retrieved from: https://www.berlingske.dk/samfund/efter-15-aar-i-blinde-under-havoverfladen-nu-skal-danmark-igen-jagte

OFS Optics, 'What is Distributed Acoustic Sensing (DAS)?', n.d., retrieved from: https://www.ofsoptics.com/what-is-distributed-acoustic-sensing-das/

Palmer-Felgate, A., and Booi, P., 'How resilient is the global submarine cable network?', *SubOptic*, 2016, pp. 1–7

Palmer-Felgate, A., Irvine, N., Ratcliffe, S., and Bah, S. S., 'Marine maintenance in the zones: A global comparison of repair commencement times', *Suboptic Conference: From Ocean to Cloud*, 2013, pp. 1–6, retrieved from: https://www.suboptic.org/wp-content/uploads/2014/10/MS02_Poster_78.pdf

Paximadis, K., and Papapavlou, C., 'Towards an all New Submarine Optical Network for the Mediterranean Sea: Trends, Design and Economics', *12th International Conference on Network of the Future (NoF)*, 2021, retrieved from: https://doi.org/10.1109/NoF52522.2021.9609879

Permanent Structured Cooperation, 'Harbour and Maritime Surveillance and Protection (HARMSPRO)', European Union, n.d., retrieved from: https://pesco.europa.eu/project/harbour-and-maritime-surveillance-and-protection/

Permanent Structured Cooperation, 'Maritime (Semi-) Autonomous Systems for Mine Countermeasures (MAS MCM)', European Union, n.d., retrieved from: https://www.pesco.europa.eu/project/maritime-semi-autonomous-systems-for-mine-countermeasures/

Permanent Structured Cooperation, 'Maritime Unmanned Anti-Submarine System (MUSAS)', European Union, n.d., retrieved from: https://www.pesco.europa.eu/project/maritime-unmanned-anti-submarine-system-musas/

Pirio, F., and Thomine, J. B., 'The Sea-Me-We 3 undersea cable system', *Optical Fiber Communication Conference and Exhibit. Technical Digest Conference Edition*, 1998, pp. 273–274, retrieved from: https://doi.org/10.1109/OFC.1998.657395

Portugal News (The), 'Portugal's navy keeps watchful eye as Russian war fleet cruises past coast', 26 Janury 2017, retrieved from: https://www.theportugalnews.com/news/portugals-navy-keeps-watchful-eye-as-russian-war-fleet-cruises-past-coast/40867

Pousson, J., 'Guerre en Ukraine : la Russie peut-elle vraiment couper Internet en Europe?', *Le Parisien*, 4 March 2022, retrieved from: https://www.leparisien.fr/high-tech/guerre-en-ukraine-la-russie-peut-elle-vraiment-couper-linternet-en-europe-04-03-2022-2EAN5SVMKJDCTDFB5GVAZY22SY.php

Public-Private Analytic Exchange Program (AEP), 'Threats to Undersea Cable Communications', *Department of Homeland Security*, 28 September 2017, retrieved from: https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf

Qiu, W., 'Submarine Cables Cut after Magnitude - 9.0 Earthquake and Tsunami in Japan', *Submarine Cables Network*, 12 March 2011, retrieved from: https://www.submarinenetworks.com/news/cables-cut-after-magnitude-89-earthquake-in-japan

Ralby, I., 'Briefing on Undersea Cables Expert Meeting', *Vulnerabilities to Undersea Data Cables*, UNODC, January 2019

République Française (La), 'Actualisation Strategique 2021', 2021, p. 18, retrieved from: https://www.defense.gouv.fr/dgris/presentation/evenements/actualisation-strategique-2021

République Française (La), 'French Seabed Strategy', 2021, retrieved from: https://www.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf

République Française (La), 'Revue stratégique de défense et de sécurité nationale', 2017, retrieved from: https://www.diplomatie.gouv.fr/IMG/pdf/2017-rs-def1018_cle0b6ef5-1.pdf

Sanger, D. E., and Schmitt, E., 'Russian Ships Near Data Cables Are Too Close for U.S. Comfort', *The New York Times*, 25 October 2015, retrieved from: https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0

Schaller, C., 'Streit im östlichen Mittelmeer – Griechenland, Türkei, Zypern. Eine seevölkerrechtliche Einordnung', *Deutsches Institut für Internationale Politik und Sicherheit*, 2022, retrieved from: https://doi.org/10.18449/2022S02

Scott, K., 'Laws governing undersea cables have hardly changed since 1884 – Tonga is a reminder they need modernizing', *The Conversation*, 21 January 2022, https://theconversation.com/laws-governing-undersea-cables-have-hardly-changed-since-1884-tonga-is-a-reminder-they-need-modernising-175312

Seibt, S., 'Threat looms of Russian attack on undersea cables to shut down West's internet', *France24*, 23 March 2022, retrieved from: https://www.france24.com/en/europe/20220323-threat-looms-of-russian-attack-on-undersea-cables-to-shut-down-west-s-internet

Shen, H., 'Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative', *International Journal of Communication*, Volume 12, 2018, pp. 2683-2701, retrieved from: https://ijoc.org/index.php/ijoc/article/view/8405

Sherman, J., 'Cord-cutting, Russian style: Could the Kremlin sever global internet cables?', *The Atlantic Council*, 31 January 2022, retrieved from: https://www.atlanticcouncil.org/blogs/new-atlanticist/cord-cutting-russian-style-could-the-kremlin-sever-global-internet-cables/

Sherman, J., 'Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security', *Atlantic Council*, 2021, p. 12, retrieved from: https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf

Sherman, J., 'The US-China Battle Over the Internet Goes Under the Sea', *Wired*, 24 June 2020, retrieved from: https://www.wired.com/story/opinion-the-us-china-battle-over-the-internet-goes-under-the-sea/

Shvets, D., 'The International Legal Regime of Submarine Cables: a Global Public Interest Regime', *PhD thesis*, 2020, retrieved from: https://www.tesisenred.net/bitstream/handle/10803/671344/tds.pdf?sequence=1&isAllowed=y

Singh, A., 'Deciphering Grey-Zone, Operations in Maritime-Asia', *Observer Research Foundation*, 2018, retrieved from: https://www.orfonline.org/wp-content/uploads/2018/08/ORF_SpecialReport_71_Grey-Zone_3N.pdf

Soames, N., 'Evolving Security in the North Atlantic', *NATO Defence and Security Committee (DSC), Sub-Committee on Transatlantic Defence and Security Cooperation (DSCTC)*, 13 October 2019, retrieved from: https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20138%20DSCTC%2019%20E%20fin%20-%20EVOLVING%20SECURITY%20IN%20THE%20NORTH%20ATLANTIC.pdf

Sprenger, S., 'Estonian intelligence flags Russian civilian vessels as would-be spy ships', *Defense News*, 13 March 2019, retrieved from: https://www.defensenews.com/global/europe/2019/03/13/estonian-intelligence-flags-russian-civilian-vessels-as-would-be-spy-ships/

Stato Maggiore della Marina, 'Marina Militare Linee di Indirizzo Strategico', *Rivista Marittima*, 2019, retrieved from: https://www.marina.difesa.it/media-cultura/editoria/marivista/Documents/supplementi/Linee_indirizzo_strategico_2019_2034.pdf

Strickland, E., 'Why the Japan earthquake didn't take down the country's internet: The undersea cable network that connects Japan to the world is damaged, but working', *IEEE Spectrum*, March 2011, retrieved from: https://spectrum.ieee.org/why-the-japan-earthquake-didnt-cripple-the-countrys-internet

Submarine Telecoms Forum, 'Industry Report 2021/2022', 2021, retrieved from: https://subtelforum.com/products/submarine-telecoms-industry-report/

Submarine Telecoms Forum 'Submarine Cable Almanac', Issue 41, May 2022, retrieved from: https://subtelforum.com/products/submarine-cable-almanac/

Submarine Telecoms Forum, 'SubTel Cable Map', 2020, retrieved from: https://subtelforum.com/cablemap/

Swinhoe, D., 'What is a submarine cable? Subsea fiber explained', *Data Center Dynamics*, 26 August 2021, retrieved from: https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber-explained/

TeleGeography, 'Submarine Cable Frequently Asked Questions', n.d., retrieved from: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

TeleGeography, 'Submarine Cable Map', 2021, retrieved from: https://www.submarinecablemap.com/#/

Truver, S. C., 'Mines and Underwater IEDs in U.S. Ports and Waterways. Context, Threats, Challenges, and Solutions', *Naval War College Review*, *61*(1), 2009, pp. 1–12, retrieved from: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1756&context=nwc-review

United Nations Convention on the Law of the Sea, Article 21(c), 1982, retrieved from https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United Nations Convention on the Law of the Sea, Article 113, 1982, retrieved from https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

UNODC, 'Key actions to protect submarine cables from criminal activity identified at UNODC global expert meeting', 7 February 2019, retrieved from: https://www.unodc.org/unodc/en/frontpage/2019/February/key-actions-to-protect-submarine-cables-from-criminal-activity-identified-at-unodc-global-expert-meeting.html

U.S. Department of State, 'The Clean Network', n.d., retrieved from: https://2017-2021.state.gov/the-clean-network/index.html

Von der Leyen, U., 'A Union that Strives for more. My agenda for Europe', *European Commission*, 2019, retrieved from: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf

Whittaker, A., 'Connected Ireland: How subsea fibre optic cables help to drive our social, economic and industrial development', *Engineers Ireland*, 13 November 2020, retrieved from: https://www.engineersireland.ie/Engineers-Journal/More/Sponsored/connected-ireland-how-subsea-fibre-optic-cables-help-to-drive-our-social-economic-and-industrial-development

Will, L., 'Conflict in the Eastern Mediterranean: Turkey Clashes with Neighbors Over Offshore Gas Reserves', *The Yale Review of International Studies*, November 2020, retrieved from: http://yris.yira.org/comments/4477

Winseck, D., 'The Geopolitical Economy of the Global Internet Infrastructure', *Journal of Information Policy,* Vol. 7, 2017, pp. 228–267

Yincan, Y., Xinmin, J., Guofu, P., and Wei, J. (Eds.), 'Safety of Submarine Optical Cable', *Submarine Optical Cable Engineering*, 2018, pp. 235–257, retrieved from: https://doi.org/10.1016/B978-0-12-813475-7.00008-4

Zan, T. de, Giacomello, G., and Martino, L., 'Italy's Cyber Security Architecture and Critical Infrastructure', in *Routledge Companion to Global Cyber-Security Strategy*, 2021, retrieved from: https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-12/italy-cyber-security-architecture-critical-infrastructure-tommaso-de-zan-giampiero-giacomello-luigi-martino?context=ubx&refId=bf424567-4e3f-496a-89ef-a0833f4d273e

Annex II - List of consulted organisations

- Danish Subsea Cable Protection Committee
- European External Action Service
- European Fishery Control Agency
- European Maritime Safety Agency
- European Subsea Cable Association
- European Union Agency for Cyber Security
- Frontex
- Government of Croatia
- Government of Denmark
- Government of Estonia
- Government of France
- Government of Ireland
- Government of Italy
- Government of Malta
- Government of Portugal
- Government of Spain
- Independent Expert Cable Repair Industry
- Independent Expert Denmark
- Independent Expert Estonia
- Independent Expert European Cyber Security
- Independent Expert European Foreign and Security Policy
- Independent Expert European Maritime Security
- Independent Expert France
- Independent Expert Ireland
- Independent Expert Italy
- Independent Expert Malta
- Independent Expert Portugal
- Independent Expert Spain
- NATO
- NATO Maritime Security Centre of Excellence

PE 702.557
EP/EXPO/SEDE/FWC/2019-01/LOT4/1/C/12

Print ISBN 978-92-846-9519-5 | doi: 10.2861/024885 | QA-07-22-441-EN-C
PDF ISBN 978-92-846-9518-8 | doi: 10.2861/35332 | QA-07-22-441-EN-N