Co-funded by the
Erasmus+ Programme
of the European Union

SECURITY
threats identification
and defence strategies

III EDITION
2022-2023

PROPOSAL:

# SEA-BER

Strengthening European autonomy,
Building European resilience

**Participant #1**
- **Name: Antoine Lebret**
- **University: Sciences Po Lille**
- **Country: France**

**Participant #2**
- **Name: Sarah Joron**
- **University: Sciences Po Lille**
- **Country: France**

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

SCIENCES PO LILLE.

# SEA-BER

## Strengthening European autonomy, Building European resilience

**European Defence Challenge III: threat identification and defence strategies**

**Authors: Antoine Lebret & Sarah Joron**

# Subject/title: SEA-BER (Strengthening European Autonomy, Building European Resilience

## EXECUTIVE SUMMARY:

Improving **European resilience to cyber threats** is one of the strategic objectives of the decade. However, **submarine cables** are often a neglected aspect of the measures in place. Yet, their importance is central as they are the backbone of the cyber infrastructure. This project aims to **improve the European response** by proposing the development of **SEA-BER software** to **map** cables and the damage that can occur. This tool should help to **reduce accidents**, the main source of cable damage, but also to **identify and prevent the threats** surrounding the physical materialization of cyber. In order for the SEA-BER software to achieve these objectives, we also propose a **set of recommendations** to adapt the technology to the legal, political and security framework.

## Table of contents

## **OUR GOAL**:
## Strengthening European submarine cables' system resilience and Defense

## OUR SPECIFIC OBJECTIVES

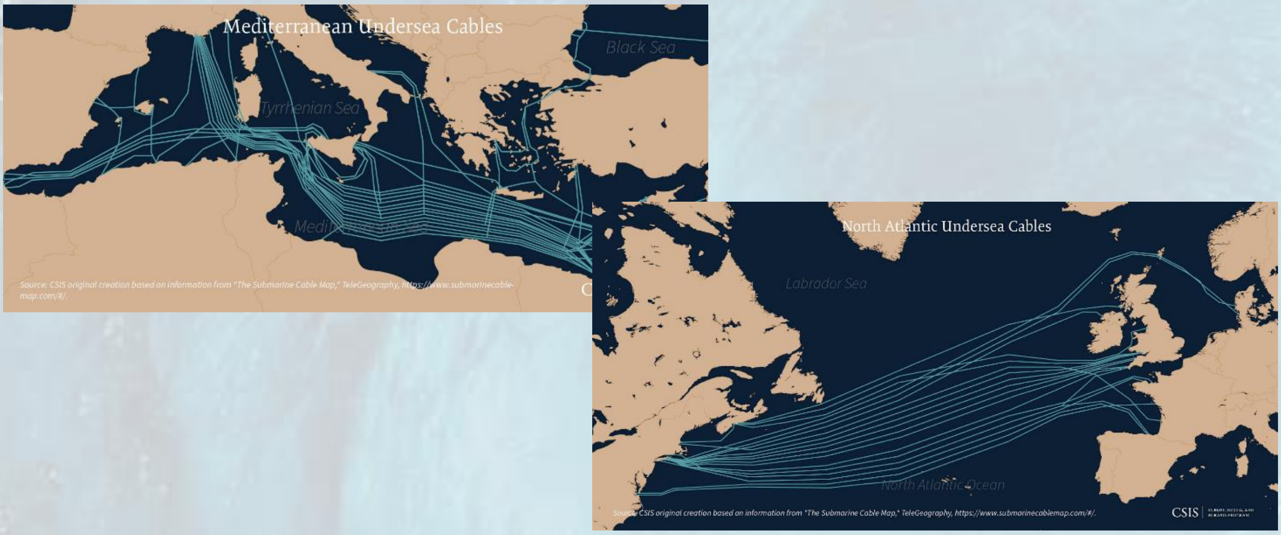
- Developing a clear European strategy among submarine cables protection
- Improving European coordination
- Raising awareness on submarine cables functions, issues and challenges
- Mitigating the risk of: deterioration, attack, surveillance
- Deepening public-private partnerships
- Reinforcing control mechanisms

# Introduction

Submarine cables in **key numbers**:

- **99%** of Internet traffic travels through the seabed
- More than **400** submarine lines, for **1.3 billion** kilometers of cable; **250** connect the EU
- **10 trillion** dollars' worth of transactions per day transiting through submarine cables
- Approximately **100 cable** breaks per year**, more than 60%** of which are human accidents often linked to fishing activities

[1]



Source: CSIS original creation based on information from "The Submarine Cable Map," TeleGeography, https://www.submarinecable-map.com/#/.

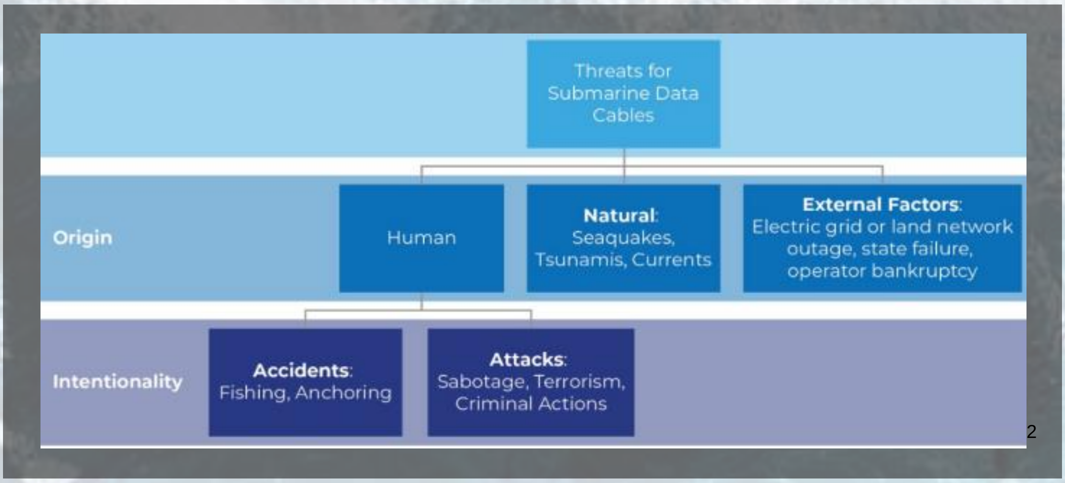
Source: CSIS original creation based on information from "The Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/#/.

*Geographical representation of submarine cables connections in Mediterranean and North Atlantic*

While this issue may seem secondary at first glance, it is in fact **essential for the European Union** to take a stand and commit itself to securing these cables. In 2015, Algeria was deprived of Internet access due to damage to the Sea-Me-We 4 cable that connected it to the rest of the world. These submarine cables are the **physical embodiment of virtual data** that travels from one corner of the

[1] Wall, C., Morcos, P. "Invisible and Vital: Undersea Cables and Transatlantic Security", *Center for Strategic and International Studies*, June 11, 2021.

world to another. This data is **civil, financial, or military and strategic**. **Identifying the threats** around this issue **and providing clear, effective, and strategic responses** is therefore an imperative to improve European governance of cable protection and resilience. Cable failures can have several causes:


Threats for Submarine Data Cables
Origin
Human
Natural: Seaquakes, Tsunamis, Currents
External Factors: Electric grid or land network outage, state failure, operator bankruptcy
Intentionality
Accidents: Fishing, Anchoring
Attacks: Sabotage, Terrorism, Criminal Actions
[2]

In all cases, the impact of the breakage or damage of one or more cables is serious, as the resulting network outages **can affect military and national security communications, cause major economic losses**, and **major disruptions to European interests**.

According to a Joint Communication to the European Parliament delivered on 16/12/2020[3] presenting the "EU's Cybersecurity Strategy for the Digital Decade "The EU lacks collective situational awareness of cyber threats". This Joint Statement guarantees the access to the Internet. To do so, **every weak part of the cyber structure must be considered**; among them the question of the submarine cables. All the issues related to the security of the European Union's submarine connections have also been raised by a more recent report, published in April 2022[4] providing a large and complete presentation of the topic. Clearly, by stating that the "European governance of cable protection and resilience still lags behind and needs improvement", it seems clear that this issue is a major concern today among European authorities.

In a context where the quest for "strategic autonomy" and the search for security unveiled by the Common Security and Defence Policy **(CSDP)** call for immediate action, the issue of cable security can no longer be left aside. Too much neglect could, in the long run**, affect European vital interests**.

Thus, the challenges raised by submarine cables for European security are:

- **Securitizing the information** conveyed through these cables. As cables have multiple use**, better protecting the cables** will mean protecting from the data of a European citizen to the top-secret military information.
- Better **protect** the weak part of the cyber infrastructure, **landing stations**.
- **Avoiding surveillance and interference** is another major issue raised recently by Edward Snowden's revelations. He denounced the Upstream and Tempora NSA's programs that allowed the United States to catch data through the cables.
- **Preventing the risk** of intentional & unintentional damages.

[2] Bueger, C. *Security threats to undersea communications cables and infrastructure – consequences for the EU,* April 2022. P22.
[3] Joint Communication to the European Parliament and the Council. *The EU's Cybersecurity Strategy for the Digital Decade*. December 16, 2022.
[4] Bueger, C. *Security threats to undersea communications cables and infrastructure – consequences for the EU*. April 2022.

# 1. Context

A closer look to **submarine cables protection** highlights several **needs and concerns** for European countries. We are here providing further examination of the **empirical and legal framework** on this subject.

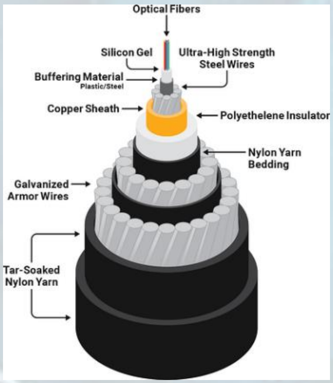
### *A. EXISTING REGLEMENTATION AND REFERENCE DOCUMENTS.*

Pre-existing standards serve as a reference framework for the protection of the underwater digital infrastructure:

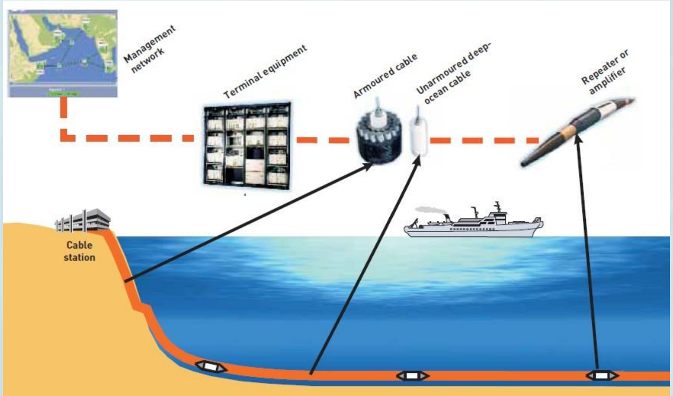
- The **United Nations Convention on the Law of the Sea (UNCLOS)**, on its article 21.C, states that the Coastal States may (but are not obliged to) adopt law and regulations related to the protection of cables and pipelines, over their respective territorial sea. States also bear responsibility for damage caused by one of their nationals. (Article 113). Thus, states bear responsibility for the protection of cables within their territorial waters, while the status of cables deployed beyond remains ambiguous. This legal framework suffers from several flaws, and fails to address some crucial issues: for example, it does not explicitly prohibit the targeting of submarine cables in the context of war.
- The **European Electronic Communication Code (directive 2018/1972)**, states that telecom providers are obliged to report incidents that had a significant impact on the operation of networks or services to their competent national authorities.
- The **Directive 2009/140/EC** of the European Parliament and of the Council "MS shall ensure that undertaking providing publics communications networks or publicly available electronic communications services take appropriate technical and organizational measures to appropriately manage the risks posed to security of networks and services […] and take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply services provided over those networks".
- Moreover, the whole EU strategic thoughts are established and detailed within the Joint Communication to the European Parliament delivered on 16/12/2022[5], presenting the **EU's Cybersecurity Strategy for the Digital Decade**.

As quickly pointed out, we can see that the current legal framework is **not properly tackling this issue** and **major ambiguities** are remaining.

### *B. MAIN CHARACTERISTICS OF THE SUBMARINE CABLES INFRASTRUCTURE*



[6]



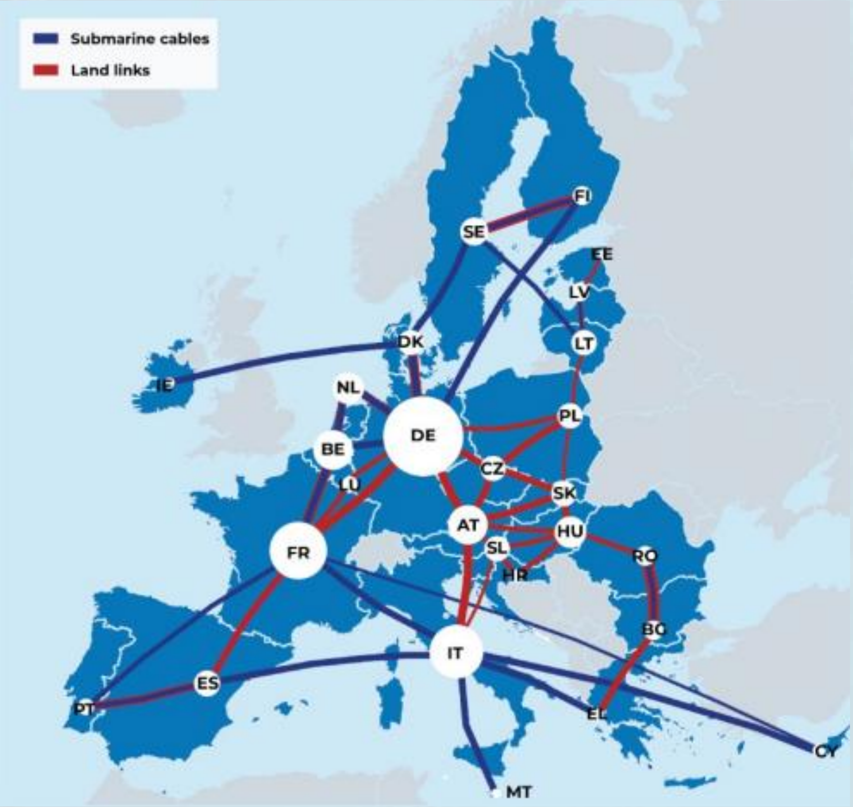
[5] Joint Communication to the European Parliament and the Council. *The EU's Cybersecurity Strategy for the Digital Decade*. December 16, 2022.

[6] Submarine Cable FAQs, *TeleGeography*, https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

*The detailed structure of a submarine cable (left) and the organisation of the different cable infrastructures (right) are shown above. In particular, the document states that submarine cables are reinforced at the sides to protect them. Offshore, although the device is robust, it can be more easily damaged, especially by ship anchors*[7].

*About the general organization of submarines cables system:*

- The **coastal countries of the Union** host major facilities. The port of Marseille is the hub of several cables connecting the EU to North African and Asian countries. The ports of Calais, Oostende (Belgium), Zandvoort (Netherlands), Genoa and Hamburg, for example, are concerned by similar systems.
- This is a maritime issue, but one that **concerns the whole of Europe**, including its territories. Most of the Union's coastal States have landing points, especially France, the Netherlands and Italy. However, the circulation of information knows no borders. **Data centres and Internet Exchange Points** are spread across several territories in Europe, including continental Europe. It is estimated that **each non-maritime State** of the Union has **4 to 5 cross-border cable systems**.
- Cables connecting to the terrestrial network of local operators cross "**Landing points**". Those structures are spread throughout almost all coastal areas over the continent, and generally host servers, routing and switching devices. Thus, as **critical strategic structures**, they tend to be physically protected, so is their exact localization. Nevertheless, it remains quite easy thanks to satellites and digital maps to locate them, which is causing several issues.



[8]

[7] Wang, C. Essay about Submarine Cables System, Fiber Transceiver Solution, October 16,2014. https://www.fiber-optic-transceiver-module.com/essay-about-submarine-cables-system.html

[8] Bueger, C. *Security threats to undersea communications cables and infrastructure – consequences for the EU,* April 2022. P18.

Furthermore, the protection of submarine cables is divided into several strands of action, which can be examined from a legal point of view.

- **The commissioning of cables, laying and maintenance activities**. The laying of new cables and their maintenance remains tightly controlled by private investors, with governments generally able to support, or oppose, projects that they do not initiate. Fleets of cable-laying vessels are also chartered and maintained by private operators, although the responsibility for the protection of the cables lies with the states, which can hire security personnel.
- **Monitoring and incident detection**. As already mentioned, the protection of submarine cables is not clearly framed by a mandate given to a State or to the European Community. Outside territorial waters, the location of the cables is no longer known, making it even more difficult to monitor them.

### *C. AN ISSUE PARTIALLY AND INADEQUATELY ADDRESSED BY THE EU*

Submarine cables are a global concern, already partially and inadequately addressed by the EU's political and legal architecture.

For years now, the European institutions have understood the crucial importance of legislating on issues of such concern as the security of information systems or cyber defence[9], particularly in the broader context of European "strategic autonomy". In this framework, **challenges related to the surveillance and protection of the undersea digital infrastructure were addressed only as factorial components of other more immediate and institutionalized threats**. A relevant example of this trend was seen on 23 April 2022, as a parliamentary question by MEP Emmanuel Maurel to the Commission focused on the EU's ability to protect its submarine cable network from intentional attacks or spying[10]. By referring his auditor to the documents on the European Cyber Security Strategy and the EU Strategy for a Global Gateway, Thierry Breton's response, on behalf of the European Commission, highlighted the **difficulty for EU authorities to consider this issue as a core strategic and security priority**.

In fact, submarine cables **are not the subject of neither strong Community attention, nor strategic thinking**. As we have seen, the deployment of new cables and the detection of faults are **primarily dependent on the prerogatives of the private sector and the States**, which are individually responsible. However, there are Community services that could be competent in various respects to work on this issue.

- The European Fisheries Control Agency.
- The European Maritime and Safety Agency (especially due to its involvement in developing the Common Information Sharing Environment (CISE)).
- FRONTEX.
- The European Union Agency for Cybersecurity (ENISA), which gained crucial status with the adoption of the EU Cybersecurity Act in 2019.

However, there is **no cooperation or coordination body** as such, as the issue of cables is considered and tackled transversally by all these actors. In practice, there is **no mandate defining the action of these agencies** in terms of surveillance or protection, which constitutes **a loophole in the Union's security and political system**.

**BETTER COORDINATION IS URGENTLY NEEDED**

[9] Joint Communication to the European Parliament and the Council. *The EU's Cybersecurity Strategy for the Digital Decade*. December 16, 2022.

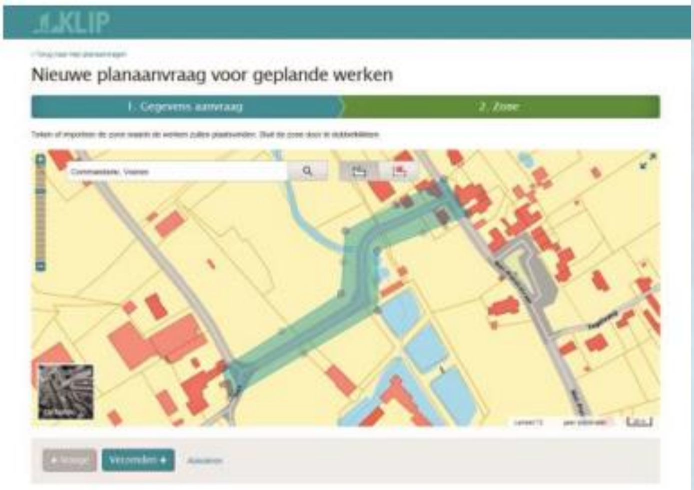
[10] See : Question for written answer E-0010219/2022 : “Submarine cables and digital sovereignty”, 23.3.2022, https://www.europarl.europa.eu/doceo/document/E-9-2022-001219_EN.html

# 2. The SEA-BER: innovation for better protection

Following the previous assessment, innovating to strengthen European Internet network is a necessity. The main objective is to improve the threat-identification and reduce the vulnerability of the submarine cables infrastructure. To do so, developing an automated information system appears to be an effective solution.

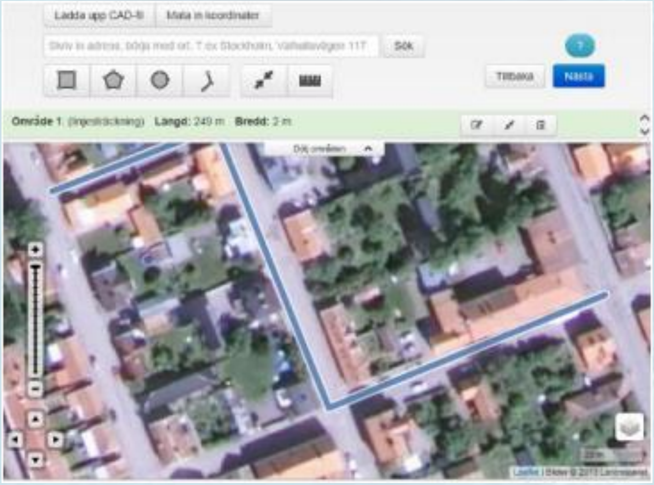
## *A. SEA-BER: A SHARED AND INTERACTIVE PLATFORM TO PROTECT CABLES*

The main objective of this innovation is to **develop a digital map to locate the cables and prevent them from being damaged**, but also to **register cable cuts**. This will allow a better understanding of the risky areas. Already existing automated information exchange tools can inspire such a software, just like KLIP (Belgium), LER (Denmark), KLIC (Netherlands), or Ledningskollen (Sweden).[11] These systems were used for terrestrial cables, suggesting that it will be easy to duplicate the concept for the subsea cables. Below are two screenshots of the Dutch and the Swedish software. The report published by ENISA, named “Protection of Underground Electronic Communications provide further details about the different available features and the challenges they faced.



*a)KLIP*

*b) Leningskolle*



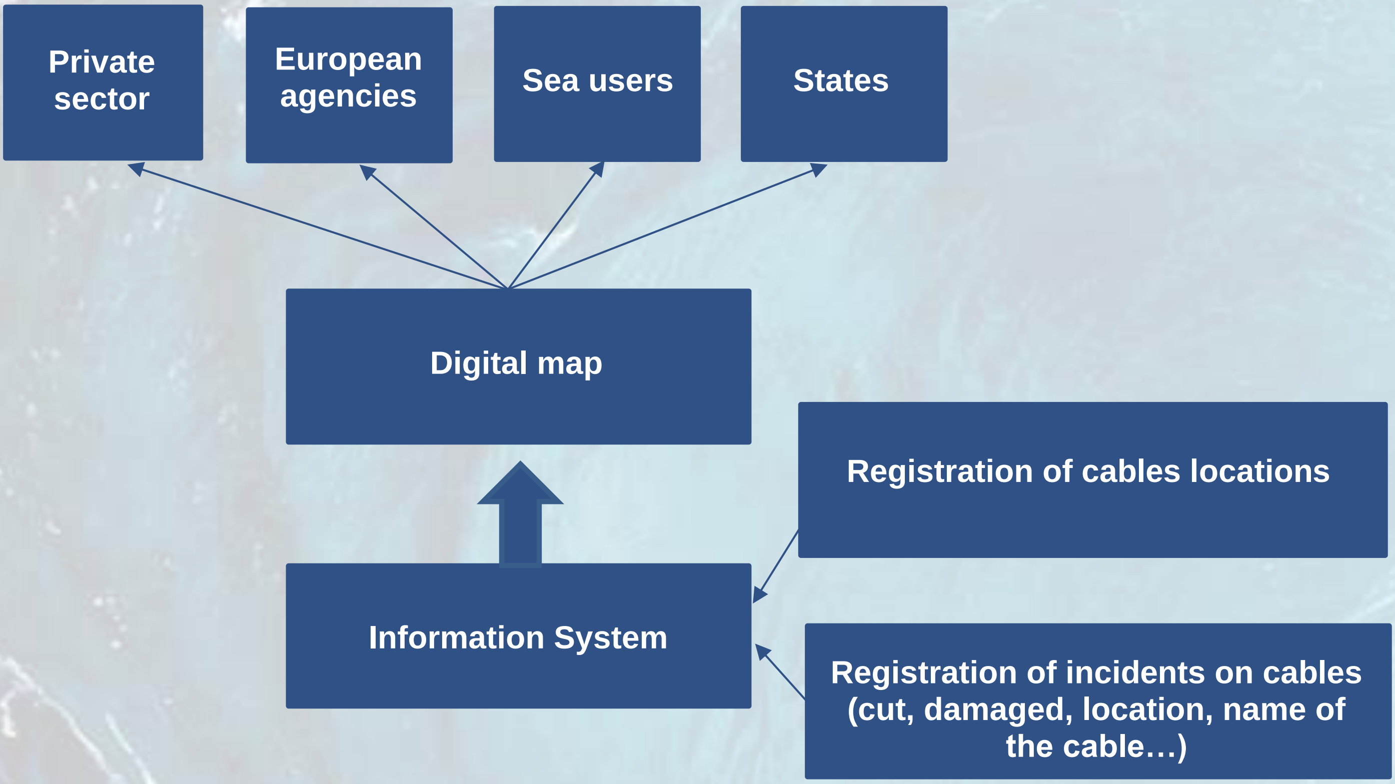
If it is easier to develop such technologies for terrestrial cables, existing technologies must be used to adapt it to the submarine environment. **Distributed acoustic sensing** is a technology that enables

[11] ENISA , *“Protection of Underground Electronic Communications Infrastructure”*. [Report/Study], December 2014 https://www.enisa.europa.eu/publications/protection-of-underground-infrastructure

continuous **real-time measurements** along the entire length of a fibre optic cable[12]. It is a key instrument for the operating industry to **determine when and where a damage** happened on the cable. Linking the software with this technology will then enable, in coordination with the private sector, to provide the software with relevant data. This data will enable **to identify the areas where recurrent damage occurred** and **deploy the appropriate measures of protection and surveillance**. The actual mapping realised by the website submarinecables.com is a good example of what the software interface can look like. The localisation of the cables is not accurate, but the graphic representation offers an **user-friendly platform**. The **European Electronic Communication Code** (directive 2018/1972) will be a useful framework for the implementation of the software. As mentioned above in 2.A., this directive obliges telecom providers to report incidents that had a significant impact on the operation of networks or services to their competent national authorities.

The software will consist in a platform where **all the stakeholders concerned will register**. **Private firms**, (maintenance, cables constructors, telecom agencies, cables owners etc.), the relevant **European agencies** (mainly EMSA, ENISA, EFCA, Frontex), **the sea users** (fishers, commercial ships etc.) and **States** will have access to different features of the platform. The **access** will, particularly, be **limited for the sea users** to guarantee the protection of cables against sabotage, terrorism or criminal activities. Providing them with the knowledge of approximate cable locations is nevertheless important as, to date, **sea users** are the **main responsible for cable cuts** because of anchoring, bottom-tending commercial fishing equipment and related dredging. At the same time, thanks to the distributed acoustic sensing technology, the damage will be mapped, and quick answers will be favoured. The **cooperation of the private sector is central** for the cable location registration.

**THE SOFTWARE**


Private sector
European agencies
Sea users
States
Digital map
Registration of cables locations
Information System
Registration of incidents on cables (cut, damaged, location, name of the cable…)

[12] *What is Distributed Acoustic Sensing (DAS)?* OFS March 30, 2020. https://www.ofsoptics.com/what-is-distributed-acoustic-sensing-das/

### *B. A SECURED AND SUSTAINABLE TOOL*

This software is therefore a **predictive, preventive and informative tool**. However, due to the sensitive nature of the information accessible, it is absolutely necessary to **secure access** to the software and to **control the information accessible** to each user. Thus, as mentioned above, different types of users will have access to different interfaces with **information filtering**. The details of each interface must be decided in consultation with the States, the private sector and the European agencies. Likewise, the conditions for registration to the software must ensure an optimal level of security. For example, it is necessary to **exclude from the software military or national security infrastructures** of Member States. Vessels should be aware that they are in an approximate area where submarine cables are present, thus inviting them to be more vigilant. The exact location is a strategic matter, and this information should remain in the hands of the competent authorities.

On the other hand, for this software to be useful in identifying threats to the cable infrastructure, it **must be used by a significant number of users**. This requires the software to be **easy to use**. Graphical representation with a digital map is the best tool and would work like a GPS that would issue an alert message near the location of cables. Software that is too complex would be left out and the benefits of the platform would be lost. This is also why a **user support service** must be put in place to ensure that the software works properly and that the various functions offered are accessible. This service is all the more useful for the private sector, which will be able to provide information on the location of its cables, but also for the competent European agencies, which will be able to set up a system aimed at **monitoring areas at risk** if necessary, **in cooperation with the EU Member States**.

Finally, to **ensure the sustainability of the platform**, the modalities of access will have to be discussed during consultation processes. Fees for access to the platform could be envisaged but, unless its use is made compulsory by a regulatory provision, there is a risk that few users will sign up. Thus, making access to the platform free of charge for users would be a better solution to ensure that the objectives are achieved in an optimal way. A European funding program or a partnership with the private sector could be envisaged. Similarly, **at least annual maintenance** of the platform should be ensured to ensure its sustainability.

### *C. LESS FAILURES, MORE CONTROL: THE BENEFITS OF SEA-BER*

This software thus offers a number of significant benefits in the European objective of protecting its cyber structure. The main benefits of the software are:

- **Rapid awareness of incidents**

Being able to know instantly where a cable break occurs will also facilitate the repair of the damaged structure and the protection of the area while waiting for the arrival of the maintenance teams, which in the European case are largely understaffed.

- **Improve the Union's predictive capabilities and identify risk areas**

Existing software is currently dependent on private structures, and everyone benefits from the information concerning their cables. As a result, the information is not centralised in any process. Bringing the information together in a single platform means that the data collected can be recorded and analysed to identify the areas where the most accidents occur. The identification of these areas will then allow for awareness-raising, prevention, surveillance and protection work where necessary. Accidents are mostly unintentional, so this is the priority cause that the software will address.

- **Reducing the number of accidents on submarine cables**

Many ships do not think about this problem. The graphical location of cables and the production of warning messages in their vicinity will raise the level of awareness of sea users and make them more attentive. This increased awareness will drastically reduce the number of damaged cables. The maintenance of a cable at sea is both time consuming due to the particular conditions of this environment and very expensive. The benefits of reducing accidents are therefore multiple, being both economic and safety related.

- **Improving public-private cooperation**

This partnership between States, European actors and private companies will allow greater cooperation in the protection of our digital infrastructures. Companies have everything to gain by taking part in this project; identifying threats will enable them to reduce their costs in the long term.

# 3. Recommendations

If the software is a necessary innovation for protecting subamarine cables and improve European resilience to cyber threats; **further efforts** remain important to **adapt the greater environment** and **make it compatible** with the objectives targeted with the creation of the software SEA-BER.

## *A. ENSURING A BETTER COOPERATION AND A GREATER COORDINATION*

In order to make the protection of submarine cables a major maritime security concern, the EU must support its efforts by **setting up bodies to bring together all the players concerned** (EFCA, EMSA, ENISA, Frontex, etc.). The figure below shows the **multiplicity of actors** on which the EU could rely, and the **different areas related to the submarine cable issue**. This complex environment is also an asset that **the EU should take advantage of**.

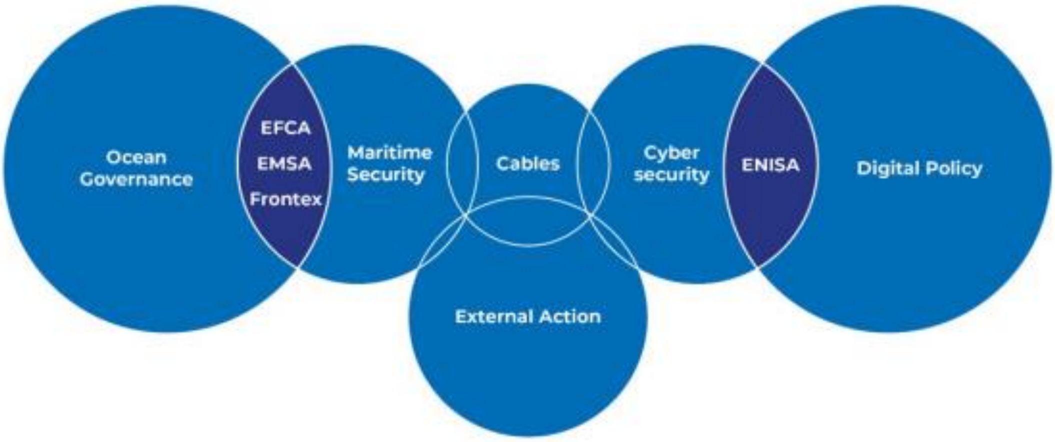


*Figure 5: Undersea cable relevant EU policies and agencies* [13]

Such a body should allow to set up a **talking space** between relevant institutions, **gather actors** whose prerogatives will be reviewed and clearly organized, and **pave the way to the definition of a common security policy**. Beyond the matter of competences, the articulation between internal and external action of the EU ought to be taken into consideration as well.

[13] Bueger, C. *Security threats to undersea communications cables and infrastructure – consequences for the EU,* April 2022. P41.

### B. DEVELOPING A SPECIFIC LEGAL FRAMEWORK DEDICATED TO THE ISSUE

Clearly, **European security ambitions** - further strengthened in recent years - and **current global legislation** - which primarily recognizes the responsibility of states, and their respective companies - are **failing to find common ground**. The European institutions must introduce Community provisions on the surveillance of submarine cables into the national law of their Member States. Such effort towards a common policy should cover both the **harmonization of monitoring procedures** - through adherence to common software, for example - and the **sharing of information** and even **maintenance capabilities**. Particular attention must be paid to compatibility with existing international regulations and legal configurations within the Member States.

The establishment of an appropriate European "legal framework" reviewing and standardizing the current one should be done in **close cooperation with**, and for, **existing European agencies**. The **mandates** of the European agencies concerned by this issue must be clarified and adapted to ensure the **distribution and integration of all the prerogatives** that will need to be implemented in support to the software. It should be possible, in the long run, to refer the matter to them. The mandate of the European Maritime Safety Agency (which is currently being reviewed) and the European Union Agency for Cybersecurity must be reviewed particularly carefully. **Avoiding duplication** and **letting no legal vacuum** is crucial.

### C. ELEVATING THE LEVEL OF AWARENESS ABOUT THE IMPORTANCE OF PROTECTING SUBMARINE CABLES

It seems clear that beyond legal considerations, **Member States still lack a strategic culture related to the issue of cables and the protection of critical infrastructures**. Thus, raising this issue everywhere as a top priority challenge should make it possible to stimulate, in the collective consciousness and in actions, the participation of everyone in this new challenge. **Within the European institutions**, it would be highly benefic to **put this issue at the agenda** of the European Commission and the European Parliament.

At present, the problem of cables is **still too marginal in European strategic thinking**. It appears as an "annex" theme in some documents, and is not even mentioned as a risk, or as an issue, in the text of the European Strategic Compass published in 2022. Clearly, this theme needs to be brought to the forefront.

This goal can be achieved in **several ways**: making cables a real concern can lead to dedicated events, or forums to exchange the subject with a large number of external actors. On a more operational level, working on organizing training sessions and exchanges between private, public and European relevant institutions could prove useful in the event of a major crisis in the coming years.

### D. IMPROVING LANDING STATIONS SECURITY

The **landing stations** constitute one of the most **vulnerable** points of the physical materialisation of the cyber. There are many such landing stations in the EU, including 12 in Marseilles, which is a hub for the arrival of submarine cables in the Mediterranean. Since the Brexit, Calais, Oostende and Zandvoort are the main arrival points for Atlantic cables. The problem with these infrastructures is that they are **not sufficiently secure**. In addition, the **software** used is in many cases **well below the security standards** that one would expect for such strategic structures. Lawfare[14] denounced this lack of precaution by pointing out the use of classic Windows or Linux programs which are easy to hack; even for beginners. However, **hacking the system** of one of these sites would have **severe consequences** as the hacker would be able to recover data, delete data but also completely cut off

[14] Hinck, G."Cutting the Cord : The Legal Regime Protecting Undersea Cables". *Lawfare*. November 21, 2017. https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables

the arrival of data by making the arrival station obsolete. Such a **"kill click"** would be dramatic. One of the recommendations made here is to **improve the resistance** of these infrastructures to such attacks. Their **physical protection** must also be strengthened because, although their exact position is not public, satellite images accessible to all can make it easy to locate them.

### *E. FOSTERING INTERNATIONAL COOPERATION*

Here again, the issues identified at the time of the establishment of the "Strategic Compass" have highlighted, once again, the **importance for** the EEAS to ramp up **cooperation with the Union's strategic partners**. Among others, beyond international organizations, cooperation on cable protection calls for even closer cooperation with certain maritime states that are particularly strategic for the Union's security. The United Kingdom and Norway to the north of the Union; and North African States and the some states of the Middle East to the south[15].

**Deepening relations with the Union's historical partners** is not the only imperative raised by the issue of cables. **Harmonizing the position and aspirations of EU countries** in terms of cyber risk protection should also make it possible to assert a **firm position regarding external players**: China - which controls several of the cables arriving on the continent with the company Huawei Marine Network - but also Russia or the United States. It should be remembered that the United States has been known to use submarine cables to spy on activities in several European states, and that China's control over several infrastructures could enable the Chinese regime to do the same. EU's cyber independence is at stake.

While the EU has been engaged in **extensive negotiations with GAFAM** on a variety of issues in recent years, consultations on legislation affecting submarine cables would be very timely. Big companies such as Google, Microsoft, or Facebook are playing a bigger role in the construction of their own cables. It is in the EU's interest to extend the legislative effort to players who control a significant part of the EU's submarine cables.

# 4. References

- Bueger, C. *Security threats to undersea communications cables and infrastructure – consequences for the EU*. April 2022.
- Hinck, G."Cutting the Cord : The Legal Regime Protecting Undersea Cables". *Lawfare*. November 21, 2017. https://www.lawfareblog.com/cutting-cord-legal-regime-protecting-undersea-cables
- Joint Communication to the European Parliament and the Council. *The EU's Cybersecurity Strategy for the Digital Decade*. December 16, 2022.
- Protection of Underground Electronic Communications Infrastructure. [Report/Study]. *ENISA*. December 2014 https://www.enisa.europa.eu/publications/protection-of-underground-infrastructure
- See : Question for written answer E-0010219/2022 : "Submarine cables and digital sovereignty", March 23, 2022. https://www.europarl.europa.eu/doceo/document/E-9-2022-001219_EN.html
- Wall, C., Morcos, P. "Invisible and Vital: Undersea Cables and Transatlantic Security", *Center for Strategic and International Studies*, June 11, 2021.
- What is Distributed Acoustic Sensing (DAS)? *OFS* March 30, 2020. https://www.ofsoptics.com/what-is-distributed-acoustic-sensing-das/

[15] Council of the European Union, "A Strategic Compass for Security and Defence", March 21, 2022, Brussels, p. 4.

ASSETs+
Alliance for Strategic Skills addressing Emerging Technologies in Defence

Co-funded by the
Erasmus+ Programme
of the European Union

# III EDITION
## 2022-2023

ASSOCIATED PARTNERS: eupportunity reportbrain

@ASSETS_Plus @ASSETs+ ASSETs_Plus_EU | www.assets-plus.eu

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.