EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 21.2.2025
JOIN(2025) 9 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

EU Action Plan on Cable Security

1. Introduction

Submarine cables, whether used for communication or energy transmission fulfil critical and strategic functions for European economies and societies. They connect several Member States to one another, islands to the EU mainland, Outermost Regions and the Overseas Countries and Territories as well as the EU to the rest of the world. Submarine communication cables carry 99% of inter-continental internet traffic. Submarine electricity cables, notably interconnectors, allow for the integration of Member States' electricity markets, strengthen their security of supply, and bring offshore renewable energy to shore. Acting on their resilience and security is necessary to protect vital strategic interests of the EU.

While submarine cables may get damaged unintentionally, the pattern observed in recent months particularly in the Baltic Sea, suggests that this critical infrastructure is increasingly the target of deliberate hostile acts. By damaging their integrity, essential functions and services are disrupted in the EU, affecting the daily lives of citizens. Such acts of sabotage – that can be elements of larger hybrid campaigns – represent a significant risk to the security of the EU and all its Member States, given the presence of submarine cables in the Mediterranean Sea, the Atlantic Ocean, the North Sea, the Black Sea and the Baltic Sea.

The security and resilience of EU submarine cable infrastructures are paramount and must be significantly enhanced[1]. On 9 February 2025, at the occasion of the Baltic Energy Independence Day in Vilnius, President von der Leyen set out four priorities to secure our critical network infrastructure focusing on prevention, detection, response and repair, as well as deterrence. This **EU Action Plan on Cable Security** designs a clear approach, based on these four priorities, to further increase the resilience and security of submarine cables, covering both communication and electricity cable infrastructure.

The capacity of the EU to prevent, detect, respond, recover and deter these incidents will show how we can meet these challenges through coordination and solidarity at EU level and in close cooperation with like-minded partners. While the protection of critical infrastructure is primarily the task of Member States, given the cross-border nature and economic relevance of submarine cables, stronger EU level action, designed to support the most impacted Member States, and complement national measures, is necessary to ensure an encompassing security approach across the EU. While this Action Plan focuses primarily on submarine cables, some of its actions could be leveraged or extended to enhance the security of other maritime critical infrastructures, such as pipelines or offshore wind fields.

This Action Plan is designed in a whole resilience cycle approach: prevent, detect, respond & repair and deter. The EU must first **prevent** disruptive incidents and increase its resilience against the threats and vulnerabilities of submarine cable infrastructures. It must also increase its **detection** capacity to be in position to identify and anticipate threats as early as possible. When an incident occurs, the EU must increase its capacity to **respond** in a coordinated way and in solidarity with the Member States most affected. In particular, the EU must develop the right capacities to recover as quickly as possible from any incident. Finally, the EU must enhance its **deterrence** posture. It will act to protect the security of critical maritime

1 See also the Commission's 2024 White Paper on "How to master Europe's digital infrastructure needs?"

infrastructure and hold malicious actors accountable, including actions against the 'shadow fleet'

This work builds on several EU activities that are already ongoing and that contribute to the security and resilience of submarine cables. These activities focus notably on building capacity (Connecting Europe Facility CEF digital and energy funding), anticipating risks (Recommendation on Secure and Resilient Submarine Cable Infrastructures[2]), adopting cybersecurity risk-management measures and reporting significant incidents (Directive on measures for high common level of cybersecurity -NIS2 Directive[3]) and enhancing the non-cyber physical resilience of critical entities (Critical Entities Resilience Directive – CER Directive[4]).

In addition, due to its clear civil-military implications, this Action Plan is conceived from the outset as an initiative that will work in full complementarity with ongoing NATO activities[5]. It will furthermore contribute to the upcoming Internal Security Strategy, the Preparedness Union Strategy and the White Paper on the Future of European Defence, putting at its core the all-hazard, whole-of-government approach recommended by the 2024 report[6] of Special Adviser Sauli Niinistö.

2. Prevention: increasing the resilience and preparedness of the EU

The first objective of the Action Plan is to reduce the number and impact of disruptive incidents and make it more difficult for any malicious actor to put the security of the Union at risk. This requires both measures to step up the resilience and security of submarine cables as well as boosting investment into the deployment of new cables.

2.1 Implementing the legal and security framework

The EU has put in place a horizontal security framework consisting of the Critical Entities Resilience Directive and the NIS2 Directive. Under the CER Directive, Member States must take measures to enhance the resilience of critical entities and the protection of critical infrastructure. This directive covers both man-made and natural risks. In particular, Member States must identify critical entities, carry out risk assessments[7] and adopt a resilience strategy. Once identified, critical entities will have to take resilience-enhancing measures such as preventing incidents from occurring, ensuring adequate physical protection of their premises and critical infrastructure, responding to, resisting and mitigating consequences of incidents, as well as recovering from incidents.

Under the NIS2 Directive, entities that are digital infrastructure and service providers operating submarine cables (such as telecommunications or digital companies) need to protect their network and information systems as well as their physical environment from any event, including man-made damage or environmental hazards. Member States are also required to include the protection of submarine communication cables in national cybersecurity strategies, mapping potential risks and mitigation measures to ensure to the highest level their protection

2 Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures (OJ L, 2024/779, 8.3.2024).

3 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

4 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

5 In line with the three Joint Declarations on EU-NATO cooperation and the agreed guiding principles enshrined in the Council and European Council conclusions

6 Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readines. Report by Sauli Niinistö, former President of the Republic of Finland, In his capacity as Special Adviser to the President of the European Commission.

7 in eleven sectors including the energy and digital infrastructure sectors

against all hazards. Given that the NIS 2 requirements are considered at least equivalent to those of CER, and in order to avoid duplication and unnecessary administrative burden on CER identified entities from the digital infrastructure sector, only NIS 2 risk-management measures and incident reporting obligations apply[8]. Incidents affecting undersea communication cables should therefore be reported to the CSIRT[9] or to the competent authority.

To increase the impact of these horizontal security framework, it is important that all actors and entities relevant to enhancing the resilience of submarine cables, are subject to security measures in an aligned and coherent way, across all Member States. To that end, the Commission encourages all Member States to ensure that **all operators of submarine communication infrastructures are covered by the national legislation transposing the NIS2 framework**. Moreover, in addition to complying with their legal obligations under the **CER Directive**, Member States are encouraged to include, in any event, entities providing essential services for submarine electronic communications and electricity transmission in their strategy for enhancing the resilience of critical entities, and in the risk assessment of essential services, as well to identify as critical the relevant entities operating this infrastructure. **Urgent and full implementation of those legal acts by Member States should be an immediate priority**.

The Commission also initiated a more targeted approach as regards submarine communication cables through its **Recommendation on Secure and Resilient Submarine Cables Infrastructures**[10]. The Recommendation provides an EU strategic policy framework to assess the risks to these communication infrastructures and to define mitigating measures. It foresees that the Commission and Member States **conduct a mapping and analysis of existing and planned infrastructures as well as regular consolidated Union-wide assessments of risks, vulnerabilities and dependencies of submarine cable infrastructures**.

In addition, the Recommendation provides for the development of a **"Cable Security Toolbox"**, setting out mitigating measures that Member States are encouraged to adopt to reduce the identified risks, vulnerabilities and dependencies. The Expert Group[11] created to deliver on the Recommendation is currently carrying out this work, **conducting risk assessments and developing risk scenarios on undersea critical infrastructures**. Once adopted, notably the risk scenarios may be regularly stress-tested. Building on the work carried out in the Nevers risk assessment,[12] the risk assessments should adopt a broad approach, also including supply chain dependencies ensuring that spare parts are provided in time and volume for the deployment of cables.

The Commission will propose **to fund preparedness testing/stress testing** of communication cables through the Cyber Solidarity Act, where a total of **EUR 30 million** is envisaged for preparedness actions in critical sectors until 2027 under the EU's Digital Europe Programme. A first call for Member States is expected this year.

Electricity cables are designed and installed for a lifetime of at least 40 years with the need for minimal interventions and include protections against fishing activities, making them already quite resilient, including through the reinforcement of cable armour and cable burial.As outlined in the 2022 Council Recommendation on a Union wide coordinated approach to strengthen the

8 As defined in Recital 20 of CER Directive

9 Cyber Security Incident Response Team

10 Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures (OJ L, 2024/779, 8.3.2024).

11 composed of the Commission, Member States and the European Union Agency for Cybersecurity (ENISA

12 Report on the cybersecurity and resiliency of the EU communications infrastructures and networks | Shaping Europe's digital future

resilience of critical infrastructure[13], the potential of conducting **stress tests** at national level should be further developed as such tests could be useful for enhancing the resilience of critical infrastructure, including submarine cables. To guarantee their security further, the **Risk Preparedness Regulation**[14] requires the identification of electricity crisis scenarios, including those resulting from malicious attacks, and the subsequent adoption of measures by Member States to prevent a crisis and to mitigate its effects should it nevertheless occur. Moreover, Member States and system operators or other energy infrastructure owners and operators should make sure that electricity cables are designed and installed in a manner that maximizes their security.

Finally, such risk assessment and stress tests should be complemented by **coordinated exercises on the security and resilience of submarine cable infrastructures**. The EU Maritime Security Strategy (EUMSS)[15] includes also a number of actions pertaining to maritime security exercises, including with the objective of enhancing surveillance and protection of critical maritime infrastructure. It foresees the participation of Member States' navies, coastguards and other relevant authorities, as well as EU Agencies. The EU will also make best use of existing exercises on maritime security and hybrid threats, in cooperation with partners, notably NATO.

2.2 An enhanced EU Investment Framework

To increase the resilience of submarine cables, it is paramount to further boost EU investment into submarine cable infrastructures, focusing on increasing cable redundancy, as well as security and repair capacities. Further efforts are needed to reduce dependencies on non-EU players - including some considered as high-risk vendors by the EU - considering the characteristics of the energy and data cables markets.

This is why the Commission will propose an **EU Investment Framework for EU cable infrastructures that are important** for the resilience and security of the EU. This investment framework will take into account economic security considerations being developed together with Member States.

2.2.1 Cable Projects of European Interest for telecommunication

Through the Connecting Europe Facility Digital programme, Europe has already an effective funding instrument for submarine communication cable infrastructures. With 30 new projects signed in December 2024, the programme now has a portfolio of **51 projects** worth **EUR 420 million**, to reinforce the Union's connectivity backbone and link the EU to partner third countries.

More specifically, thanks to these investments, the Commission has enhanced the EU presence in routes to Africa, the Middle East, in Central and Eastern Europe, in the Atlantic, and in the Nordic region, including the Baltic, where for the latter, **EUR 35.6 million** have just been invested in eight specific submarine data cables.

13 Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (2023/C 20/01) ((OJ C 20, 20.1.2023, p. 1).

14 Risk Preparedness Regulation (EU) 2019/941, OJ L 158, 14.6.2019, p.1; this regulation is currently under review.

15 Council conclusions on the Revised EU Maritime Security Strategy (EUMSS) and its Action Plan. st14280-en23.pdf

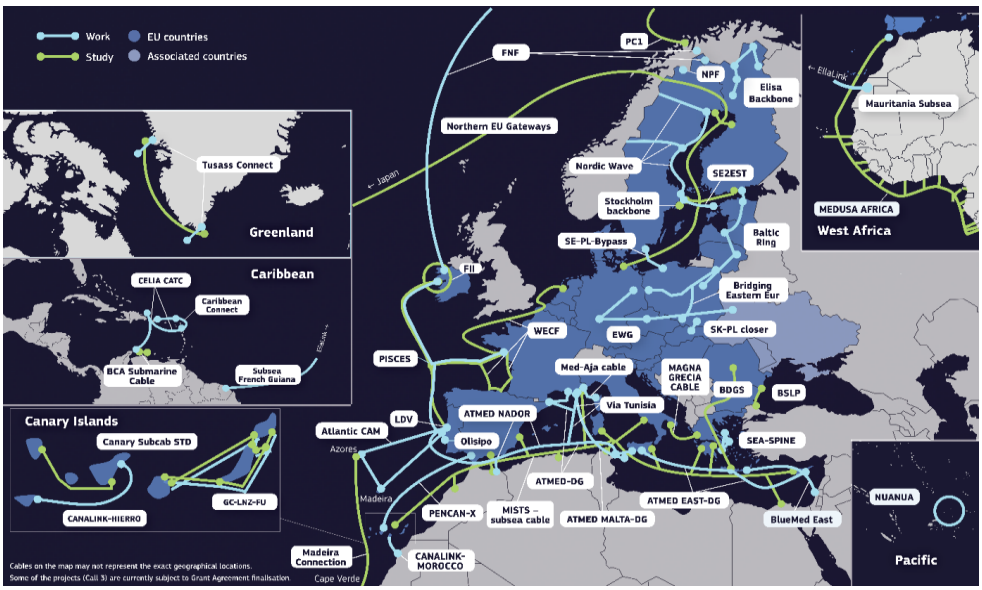

Figure: cable projects funded in calls 1-3 under the Connecting Europe Facility Digital programme. The map may evolve according to the actual implementation of the programme.

In the years 2025-2027, an additional **EUR 540 million** will be invested under CEF into digital infrastructures, including submarine cables, **totalling almost EUR 1 billion** under the current Multiannual Financial Framework.

As envisaged in the Recommendation on Secure and Resilient Submarine Cable Infrastructures, the Expert Group is expected to propose a **draft list of strategic Cable Projects of European Interests (CPEIs)**. These CPEIs could be prioritised and fast-tracked for Union funding, complemented with national funds and, where possible, with private funding, in line with the criteria under the Recommendation as well as Union funding and State aid rules. In that perspective, the Commission will review, through a Delegated Act, the CEF Regulation (Annex Part V) to create a clear framework for CEF investments in submarine cables, reflecting the priorities proposed by the Expert Group, based on a sound analysis of the actual resilience needs, for instance at level of Member States or maritime basin. It is paramount to prioritise projects which are important from a resilience and strategic standpoint, but which would unlikely be considered bankable and deployed autonomously by private investors. The **Commission will therefore launch a dedicated dialogue with industry, private investors, as well as the European Investment Bank and National Promotional Banks and Institutions** to investigate possible ways to jointly finance CPEI cable infrastructures. The intention is to agree on a contractual framework for the involvement of financial partners to combine CEF grants with non-EU budget to fund the cable infrastructures (blending facility with national fundings and private investment).

The combination of existing funds that can support digital infrastructure, including Connecting Europe Facility, Neighbourhood, Development and International Cooperation Instrument (NDICI), Instrument for Pre-accession Assistance (IPA) and the European Regional Development Fund –could be further explored. Investments under Global Gateway should also be done in such a way as to enhance the EU's resilience, especially when connecting Outermost Regions and Overseas Countries and Territories. As outlined in the Recommendation on Secure and Resilient Submarine Cable Infrastructures, this requires an alignment between different sources of financing at EU level and strong coordination, so that the EU acts in a Team Europe

approach. Concretely, this could be implemented through the coordination of investments in different segments of cables, according to the areas of competence of the relevant programmes (EU connectivity and international routes). It also applies to investments in relevant enabling frameworks (e.g. capacity-building, legal advice).

2.2.2 Electricity Projects of Common Interest and Projects of Mutual Interest

As regards electricity cables, the EU regulatory framework on Trans-European Networks for energy (TEN-E) provides for a comprehensive process for the selection of Projects of Common Interest (PCIs) and Projects of Mutual Interest, with third countries (PMIs). The EU has already selected 100 electricity PCIs and facilitated their permitting and construction, including by funding – notably CEF- Energy funds which has invested over EUR 8 billion in EU's energy infrastructure, the majority for electricity cables. The largest grants that CEF Energy has financed are the following (all in electricity):

- Baltic synchronisation: EUR 1.23 billion in total spending > EE, LT, LV, PL
- Great Sea Interconnector (subsea): EUR 658 million > CY, EL
- Bornholm Energy Island (subsea): EUR 645 million > DE, DK
- Biscay Bay (subsea): EUR 578 million > ES, FR
- Celtic Interconnector (subsea): EUR 531 million > FR, IE

Electricity infrastructure already face the compelling need to be rolled out further and faster to support EU's climate and energy objectives. In November 2023, the Commission published the EU Grid Action Plan outlining 14 non-legislative actions aimed at strengthening the investment framework for electricity grids. These actions are set to be completed by mid-2025. The EU must invest more in modernising and expanding its network of energy transmission and distribution infrastructure, accelerating investments for electricity. In the coming years, approximately EUR 530-540 billion in investments will be needed for electricity grids, averaging EUR 77 billion annually. This is significantly higher than the EUR 85 billion invested between 2021 and 2023. The European Grids Package will also aim to further facilitate investments in grid infrastructure and seek to prevent the participation of non-trusted third country players in critical electricity cables.

As regards the Baltic Sea region, the Commission has facilitated the interconnection and integration into the European energy market of Northern Europe and focused on removing the energy isolation of the Baltic States and Finland. For the past 15 years, over EUR 2.7 billion of EU funding were invested in the region in this regard. Undersea interconnectors play a key role in this energy integration and in ensuring security of supply in the region. Moreover, with an offshore renewables' potential on 91GW, the Baltic Sea will be one of the key areas for the development of the EU's offshore renewables production and infrastructure. All of this represents a major development and diversification of infrastructure with a direct impact on reducing the vulnerability of these networks

2.2.3 Smart Cables and early warning

Smart cable systems offer an interesting perspective for preventing attacks and detecting incidents. They can be used as large geographical sensor networks to monitor nearby activities, anticipate threats and vulnerabilities, acting as an early warning system to protect the cable

infrastructure itself and the surroundings, including for both civilian (e.g., environmental monitoring) and military purposes.

CEF Digital promotes smart cables in the 2024-27 work programme. The Recommendation on Secure and Resilient Submarine Cable Infrastructures also includes references to sensor and monitoring systems as well as the uptake and deployment of innovative solutions to detect and deter threats. The TEN-E Regulation also promotes cross-border smart electricity grids and CEF Energy has already facilitated funding of EUR 410 million for such projects, mostly for works.

Besides their primary use as broadband cables, smart communication cable systems can be used as backbones for connecting underwater resources such as docking stations (launch, recovery, data transfer) for uncrewed underwater vehicles and systems, to perform seabed exploration, repair functions, surveillance, etc. In the long term, the expansion of the fleet with these advanced vehicles and facilities, their interoperability with modern vessels and their operational support could be envisaged under future EU programmes.

Feasibility studies will be launched under CEF in close coordination with the European Defence Fund and the European Maritime, Fisheries and Aquaculture Fund (EMFAF). BlueInvest projects already running and addressing underwater observation, detection communication and surveillance, in particular on launch and docking solutions for Autonomous Underwater Vehicles (AUVs), as well as the use of swarm intelligence technologies. Coordination will be ensured also with relevant Horizon Europe funding, notably through a dedicated action on "preparing the advancement of the state of the art of submarine cable infrastructures".

The Commission will establish **an industry forum** to consult the most relevant players and trade associations in submarine cable technologies to **design an industrial roadmap for the deployment of surveillance and protection technologies for submarine cable infrastructures**. The Expert Group of Member States established to deliver on the Recommendation will be associated closely to this work.

Key actions on prevention

- The Commission, together with Member States and ENISA, through the Expert Group created to deliver on the Recommendation on Secure and Resilient Submarine Cable Infrastructures, will complete by Q4 2025:
    - a **Mapping** of existing and planned submarine cable infrastructures;
    - a **Coordinated Risk Assessment** (risks, vulnerabilities and dependencies) on submarine cables, taking into account spare part security of supply, and stress testing methodology;
    - a **Cable Security Toolbox** of mitigating measures;
    - a priority list of **Cable Projects of European Interest (CPEIs)**.

- The Commission will, by end of 2025, propose a Delegated Act to amend the Annex part V of the Connecting Europe Facility (CEF) Regulation to prioritise the CPEIs as CEF Projects of Common Interest. This would be a first step towards an EU Investment Framework for submarine Cable projects.

- The Commission will:
    - review the security of energy supply framework with special attention to critical energy infrastructure.
    - facilitate investments and enhance the security of critical electricity cables through the European Grids Package

Member States:

- must transpose and implement the CER and NIS2 Directives, as a matter of urgency.
- are encouraged to ensure that all operators of submarine communication infrastructures are covered by the national legislation transposing the NIS2 framework.
- are encouraged to duly consider entities providing essential services for submarine electronic communications and electricity transmission when implementing the CER directive, in particular as regards strategy, the risk assessment and the identification of critical entities.
- must make sure that electricity cables are designed and installed in a manner that maximizes their security.

3. Detection: increasing the EU's capacity to monitor and detect threats

Today, insufficient cooperation at regional, national and European level can be exploited in the context of a hybrid campaign, leveraging the fragmentation of different layers of surveillance mechanisms, allowing to evade detection and create plausible deniability. Rapid and real-time detection has proven to be one of the foundations to counter sabotage against submarine cables. The recent incidents in the Baltic Sea were detected almost in real time allowing the vessel to be stopped before further damages are done. The main challenges come from establishing intentionality as well as prediction and threat indicator analysis.

3.1 Support an Integrated Surveillance Mechanism for Submarine Cables

Today there is no capacity to effectively monitor all the dimensions of the threats surrounding submarine cables and create a single and integrated situational picture at sea basin level. To be able to issue early alerts, it is essential to make several systems work together, fusing data available at national and Union level.

The EU situational picture for the security of maritime infrastructures could benefit from the activities of several systems such as the Integrated Maritime Services[16] for maritime surveillance and situational awareness at sea, hosted in the European Maritime Safety Agency (EMSA). Other systems bring additional information, such as the MARSUR (Maritime Surveillance) network for Member States' Navies under the European Defence Agency framework for a Recognised Maritime Picture, EUROSUR, the integrated framework run by Frontex for the exchange of information and operational cooperation within the European Border and Coast Guard services as well as the voluntary Common Information Sharing Environment (CISE) for the maritime domain managed by EMSA. Connecting and fusing the capacities of all these frameworks needs to be done seeking synergies, building on already operational solutions and avoiding duplication. In addition, intelligence analysis issued by the Single Intelligence Analysis Capacity (SIAC) can also contribute and provide strategic assessment to improve broader situational awareness.

To support Member States' efforts the Commission proposes to support the development and deployment, with voluntary participation of member States, of **an Integrated Surveillance Mechanism for Submarine cables per sea basin.** The objective is to support willing Member States to link and fuse - on a trusted regional sea basin level - data coming from several sources, including EMSA, Member States, private operators, smart cables, shipping industry or defence channels. This could subsequently provide timely and accurate situational awareness for enhanced detection and monitoring, including to patrolling ships. This would allow early detection of threats with a view to shorten response time, allow remedial action (e.g. interception) and increase the capacity to attribute responsibility. While focusing primarily on submarine cables, this approach could also be leveraged to support increased surveillance and situational picture for the security of other maritime critical infrastructures such as pipelines or offshore wind fields.

Regional sea basin hubs could benefit from different services and EU instruments, such as:

- **Early detection of suspicious maritime (vessels of interest) activities** around cables (through open source and AI specific software development) based on behavioural analytics and traffic analysis available for instance in EMSA, as well as geofencing. Where agreed by participating Member States, it should be possible to integrate military surveillance systems and data.
- **Enhanced space surveillance services** closely monitoring the activity of vessels of interest through the Copernicus Maritime Surveillance service implemented through EMSA; which should involve punctual surveillance as well as having permanent/regular

16 Within the Union Maritime Information and Exchange System, regulated in the VTMIS Directive 2002/59/EC on Vessel Traffic Monitoring and Information System. IMS is EU-wide and provides cross border and cross sector information and communication.

eyes in the most sensitive regions, enabled by the new EU Earth observation governmental service

- **Dedicated surveillance services** such as drones (air, surface and underwater) with the ability to track, trace and monitor vessels of interest, especially when a suspicious activity is detected, using and expanding the capacity of EMSA to procure such services, drawing on the experience gained with rescEU[17].
- **Real-Time Network Monitoring**: using software tools like Security Information and Event Management (SIEM) systems to detect anomalies in data traffic that may indicate disruptions or unauthorised access attempts.
- **Intrusion Detection Systems (IDS)**: specialised systems to monitor physical and data-layer activities, identifying tampering or suspicious activities near landing stations or repeaters.

In addition, **SIAC will produce regular reports on suspicious vessels and threats** against the submarine cable infrastructures based on intelligence received from Member States and coordinated with and supported by the European Union Satellite Centre (SATCEN) on request of SIAC.

In the **immediate term**, it is imperative to make sure access to EMSA systems and services is available to all relevant authorities at national level. To further enhance maritime domain awareness, the Commission, in cooperation with EMSA and Member States, will investigate accelerating the deployment of the voluntary Common Information Sharing Environment (CISE) to reach its full potential, encouraging more Member States to join.

In the **short term**, it is already possible to launch **a dedicated regional integrated surveillance mechanism focusing on the Baltic Sea**. This can be done by leveraging an open call under the Digital Europe Programme (EUR 22 million) for the creation of cross border Security Operations Centres (SOCs). This **first regional surveillance hub could be a test bed for integrating all the relevant data, services, networks and entities per sea basin**. In the **medium term**, this approach could be expanded to other sea basins.

Significant resources has already been invested through the EU Framework Programme for Research, into the development of innovative detection and situational awareness technologies, available to Border Guards, Police, critical infrastructure operators and other national authorities[18]. The Commission will continue promoting the development and uptake of **technological solutions** to enhance the detection capacity of incidents and the effective use of this information. This will be stimulated by an overview report prepared by the Commission in 2025.

3.2 Civil and military approach

Ensuring a **strong civil-military approach** is essential for the effectiveness of the mechanism. Maritime domain awareness, surveillance and interdiction require state of the art naval capabilities. Member States should further invest to develop, acquire and operate such

17 the strategic reserve of European disaster response capabilities and stockpiles, fully funded by the EU under the Union Civil Protection Mechanism (UCPM).

18 Such as: underwater sensing technologies (projects SMAUG and UNDERSEC); solutions for automatic detection of abnormal vessel behaviour, especially in case of turned off or spoofed AIS (MARISA, AI-ARC, PROMENADE, EFFECTOR and COMPASS2020); early warning signals and real-time awareness (VIGIMARE).

capabilities in a coordinated manner with the support of the EU, using the European Defence Fund for R&D and the proposed European Defence Industry Programme for joint acquisition.

More concretely, the military dimension of the integrated surveillance mechanism – and in particular deploying an underwater situational awareness – could be addressed in the framework of the Defence Projects of Common Interest as proposed in the future European Defence Industry Programme. Projects to develop maritime domain capabilities under the Permanent Structured Cooperation (PESCO) and within the framework of European Defence Agency (EDA) should be accelerated.

Funding from the European Defence Fund could also be mobilised to develop national sensors for predictive threat analytics but also national Radio Frequency (RF) space-based detection capacity which could allow to detect vessels of interest faster. In this perspective, the Commission is ready to work with Member States for the deployment of a network of national undersea sensors (vibrations, pressure changes, or unusual activity near the cable), smart buoy (monitoring acoustic signatures to detect potential threats such as ship anchors), or using optical cables as a sensor (Distributed Acoustic Sensing).

The Commission will integrate space-based RF detection capacities under the EU Space Programme, complementing the use of existing devices and data from subsea operators. Subsea optical and electricity cables and offshore wind farms also offer significant opportunities for collecting undersea data. Strong cooperation between private operators and the military is key to unlocking this potential.

The **role of private entities** is paramount to increase the detection capacity. Private entities should be encouraged to enhance reporting (voluntary or regulatory) incidents. Information about these incidents, including those below the legal reporting obligation, should be shared immediately with all impacted Member States. For instance, integrating this functionality in the regional hubs would allow for a swifter response and interception and avoid further cuts and incidents by the same vessel.

Key actions on detection

The Commission, together with Member States, will:

- support the development and deployment on a voluntary basis, of an **Integrated Surveillance Mechanism for Submarine cables per sea basin** designed to link and fuse data from relevant sources and set-up accurate & real time sea basin situational picture.
- work towards the rapid establishment of a **dedicated regional hub in the Baltic Sea region as a test bed of the integrated surveillance approach**.
- explore the concept of a **network of undersea sensors** to be deployed to secure submarine cables.
- launch a **dedicated surveillance drones programme** (air, surface and underwater) to boost the development and deployment of such capacities.
- prepare a **report to promote the use of new technological solutions** for detection of cable incidents.
- support the development of public private **partnership with cable operators** in view of promoting increased voluntary reporting of cable incidents.

4. Response & Recovery: Stronger EU cooperation and solidarity

4.1 Response: towards a more coordinated crisis response

When an incident occurs on a submarine cable, several crisis frameworks could be activated. The 2024 EU Critical Infrastructure Blueprint[19] is aimed at improving EU-level coordination and response to disruptions of critical infrastructure with significant cross-border relevance, that are in scope of the CER Directive. The Cybersecurity Blueprint, which is currently under review, covers crises resulting from large-scale cybersecurity incidents that affect the availability of network and information systems for the sectors under the NIS2 Directive, including sabotage of submarine cables. Sectorial energy legislation, such as for the electricity and gas sectors, contains specific operational provisions to manage crises, involving also technical experts from Member States directly.

The recent Baltic Sea incidents have highlighted the **need for a more tailormade and coordinated response by leveraging synergies between these different crisis management frameworks**. In particular, given the specific nature of submarine cables and the civil-military by nature dimension of these incidents, it is important that Member States make effective use of the existing reporting incident mechanisms set out in the CER and NIS2 Directives.

19 Council Recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance (C/2024/4371) (OJ C, C/2024/4371, 5.7.2024)

Furthermore, Member States should use contact lists provided for in the EU Critical Infrastructure Blueprint and in the Cybersecurity Blueprint in case of incident whist ensuring that these points of contact have the necessary links to all the dimensions related to cable incidents.

Additionally, **cooperation and synergies with NATO should be stepped up**. Building on the ongoing work in the context of the EU-NATO Structured Dialogue on resilience, cooperation at staff level will be further deepened on the resilience and protection of critical submarine infrastructure, including submarine cables. Staffs will focus on promoting synergies between respective initiatives at operational level, including through exercise and scenario-based discussion, enabled by targeted information sharing and coordination in a crisis. This is all the more important as NATO is increasing activities for the maritime security in the Baltic Sea.

Finally, Member States can also access emergency assistance under the Internal Security Fund to support response such as investigation and securing the infrastructure. In case the incident on a submarine cable is part of a larger hybrid campaign, the **EU Hybrid Rapid Response Teams (HRRT)** could be deployed to support, at their request, the affected Member States.

4.2 Recovery: towards an EU Cable Vessels Reserve Fleet

When an incident on submarine cable infrastructures occurs, it is paramount to intervene rapidly and repair the damaged cable. However, while today's vessels have proven effective to repair damaged cables with reasonable response time, their current number and capacity would be insufficient to timely intervene in case of systemic and simultaneous attacks to critical cables across different maritime areas of the Union. Maintenance and repair vessels are a major bottleneck for the capacity to recover from an incident[20]. In addition, the availability of repair equipment and specialised workers is an issue, especially for specific and complex cables such as subsea electricity grids.

In the **short term**, the Commission will propose to facilitate the contracting of repair services available on the market, possibly through the Union Civil Protection Mechanism. In particular, as immediate action, modular repair equipment capacity ready to be plugged on vessels could be supported to increase the responsiveness of the EU, in a cost-effective manner.

It is equally important to ensure the security of supply of cable spare parts (e.g. gabion boxes, fencing materials or transformers for substations) and take the necessary measures to **stockpile essential material and equipment** if and where needed, so as to always be able to repair. The stockpile reserves should strategically be prepositioned in high-risk areas to ensure rapid deployment. For electricity submarine cables, given their specificity and bespoke design, efforts should be combined between Member States, cable owners and cable producers, to standardise the design requirements, spare parts (such as joints), as well as the training of repair crews.

In the **medium term**, the **Commission could support the acquisition or contracting of additional repair and deployment vessels,** possibly targeting the Baltic/North, Mediterranean and Atlantic Sea basins, prioritising the Baltic/North basin, currently being the one most affected. Adding more vessels to the current fleet would shorten the reaction time on critical submarine infrastructures affected by systemic failures. This could also take the form of a

20 This was confirmed in the Expert Group of the Recommendation on Secure and Resilient Submarine Cable Infrastructures.

regional framework agreements to secure the immediate and prioritized availability of appropriate vessels with specialized crew in case of a need to repair or deploy. A pilot regional framework agreement facilitated by the Commission could be first tested for the Baltic Sea together with Member States, cable owners and cable producers.

In the **medium term**, the Commission is proposing to establish a **multi-purpose EU Cable Vessels Reserve Fleet** to be used in case of emergency, to deploy or repair electric or optical submarine cables connecting EU territories. The vessels would have icebreaker capabilities to be able to operate in northern latitudes and in extreme weather conditions and could include modular repair or deployment equipment. They could possibly contribute to responding to other threats such as environmental ones (e.g. oil spill). EU funding, in combination with Member States' support, could be mobilised for this purpose. For instance, the fleet could be co-financed by the Connecting Europe Facility[21] in synergy with other funds, in particular cohesion funds with the interested Member States. This capacity could possibly be embedded into the Union Civil Protection Mechanism, including rescEU.

Given the EU's highly advanced industrial capabilities in building specialised vessels to maintain and repair submarine cables, this could additionally contribute to the upcoming Industrial Maritime Strategy aimed at strengthening Europe's maritime manufacturing sector.

Key actions on response and recovery

The Commission, together with Member States will:

- enhance the **effectiveness of EU's crisis response in all its dimensions** by increasing synergies with existing frameworks and assessing with Member States the need for a more tailormade approach.

- pooling budget from Union funding programmes, including the possibility for voluntary transfers by Member States from cohesion funds into CEF, to finance an increase in **EU cable vessels capacities,** as well as modular repair equipment.

- propose in the medium term – depending on the needs – to build an **EU Cable multipurpose Vessels Reserve** ready to use, possibly through an **Implementing Act under the Union Civil Protection Mechanism (including rescEU)**. This could be complemented by regional framework agreements to secure the immediate availability of appropriate vessels with specialised crews.

- **design a joint approach to ensure the security of supply of cable spare parts** through e.g. targeted stockpiles.

The Commission and the High Representative will:

- **enhance operational cooperation with NATO** on the resilience and protection of cable and other critical submarine infrastructures.

21 Under the Connecting Europe Facility, this could be funded as accompanying measure under the terms of Article 9.1 of the CEF Regulation

5. Deterrence

While all the actions listed in this Action Plan increase the resilience and response framework of the EU in case of an incident act as a deterrence, it is also important to be able to follow through when it comes to attribution (e.g forensics) and sanctions. This is especially important since most often these actions are prepared and envisaged with the objective of obstructing attribution. The EU should be equipped with the necessary means to qualify, prove, coordinate attribution and impose sanction. The EU will therefore bolster its deterrence posture by holding perpetrators accountable for their actions and raising costs for malign actors.

5.1 Responding to hybrid campaigns: raising costs for perpetrators

The EU has established a Hybrid Toolbox which provides a framework to address, in a comprehensive manner, hybrid campaigns affecting the EU and its Member States and partners. It facilitates an informed, targeted and coordinated EU-level response to such campaigns using the whole range of EU tools and measures.

Measures range from statements and joint attribution to other diplomatic measures and coordinated communication, also together with partners, including NATO. These measures aim to raise awareness about the threat landscape, hold malicious actors accountable and signal the possible consequences of their behaviour. They also aim at deterring by countering plausible deniability narratives from covert operations.

The EU should actively make best use of the existing sanctions' regimes to prevent and respond to any sabotage on submarine infrastructure. The EU can use the newly established sanction regime in view of Russia's destabilising activities. These sanctions can target those who are found responsible for implementing, supporting, or benefitting from actions or policies by Russia which are aimed at destabilising the EU, its Member States, third countries and international organisations (those listed are subject to an asset freeze and a travel ban). Furthermore, measures limiting the capacity of the "shadow fleet" to circumvent EU sanctions contribute to improving the security of the EU's maritime areas. For better effectiveness, the EU and G7 will continue to explore further options to address respective risks of the shadow fleet.

5.2 Reinforce the Union's actions against the shadow fleet

The recent incidents highlight the role and potential use of vessels which are often old, in bad shape, with obscure ownership and insurance. This fleet of aging vessels – mostly tankers and other cargo vessels operating to circumvent sanctions – represents a serious security risk for the Union, whether they are environmental risks (oil spill pollution) or risks for the critical infrastructures (cables cuts) or energy supply security risks, making it a broader geopolitical threat. Vessels of interest (i.e. those that would warrant specific attention) should also cover those engaging in unsafe operations or disguised as fishing or research vessels but equipped with surveillance gear.

Concrete actions need to be taken to reduce the possible impact of these vessels and prevent them from creating damages intentional or not in the different sea basin around the Union, in

accordance with the international law of the Sea framework[22],. The EU should work with its partners to align the different listing of prohibited vessels and ensure therefore that no loopholes are allowed.

The EU should continue and enhance the coordinated approach to strengthen further outreach to flag and port states whose vessels are suspected of damaging action in order to be able to increase accountability and responsibility.

Finally, the EU and its Member States, working together with the International Maritime Organisation, should establish a common understanding of relevant provisions of the International law of the sea enabling Member States, as coastal and flag States, to more effectively protect critical infrastructure and take action in relation to the shadow fleet of vessels and any vessels of interests operating on the high seas. In particular, the legal framework for interception or boarding of vessels representing risks for the EU should be carefully assessed, in full compliance with United Nation Conventions on the Law of the Sea (UNCLOS).

5.3 Advance cables diplomacy – working with partners

The network of cable infrastructure is intercontinental, and incidents also take place in other parts of the globe. It is therefore important to develop a strong international cooperation on cable security.

First, on the resilience of submarine cables, the EU should develop and deploy an advanced cable diplomacy. As announced in the Recommendation on Secure and Resilient Submarine Cables Infrastructures, Member States and the Union, working in a Team Europe approach and through the EU delegations, should continue to cooperate in promoting the development of secure, trusted and resilient submarine cable infrastructures with neighbouring countries, strategic partners, other third countries, and in multilateral and multistakeholder fora. For a broader impact, the principles of the EU Cable Security Toolbox will be promoted for the infrastructures managed or developed in cooperation with enlargement and neighbourhood countries (Medusa across the Mediterranean, Black Sea cables, etc.), and other third countries (BELLA with Latin America and the Caribbean, EurAfrica cable, other Global Gateway projects, etc.).

Second, when it comes to addressing incidents, the Union should enhance the exchange of information with, for instance, Indo Pacific partners who are facing similar incidents in relation to critical submarine infrastructures. This should be carried out by leveraging existing partnerships and networks to further promote initiatives related to the security, situational awareness and resilience of submarine cables and ensure that EU support to third countries is fully aligned with EU security interests. The High Representative will undertake diplomatic initiatives in multilateral fora, such as UN to raise awareness about the ongoing threats to the security interests of the EU and its Member States[23]. These issues will also be addressed in relevant **Security and Defence Dialogues** with partners and can also be covered in **Security and Defence Partnerships** as relevant. Third, work at multilateral level could also include a possible reflection on how to make full use of all possible courses of action in conformity with

22 notably UNCLOS, and the International Maritime Organization's Resolution A.1192(33) of 6 December 2023

23 This could include the ITU International Advisory Board for Submarine Cable Resilience.

the International Law of the Sea, including the UN Convention on the Law of the Sea (UNCLOS) with a view to increase the protection of submarine cable infrastructures as well as the promotion of norms and best practices.

Key actions on deterrence

The Commission and the High Representative, together with Member States will:

- deploy a **proactive cable diplomacy** to reach out to strategic partners, including in multilateral fora, with a view to cooperate on issues related to cable security.
- enhance the **capacities of the EU to react and limit the impact of the shadow fleet**.
- enhance the **capacity to hold malicious actors accountable,** notably by making best use of the existing sanctions regimes and coordinated attribution.
- step-up the **strategic communication approach** on cable security to combat the hybrid campaign abusing plausible deniability.
- launch a **reflection at international level on how to make full use of the International Law of the Sea Framework** to enhance the security of submarine cables
- reinforce **dialogue and cooperation with NATO** on cable security.

6. Conclusion

In the face of increased security threats, the EU must take swift and decisive action. Using the tools at its disposal in a more coordinated and effective manner, the EU can set a powerful example of solidarity and unity.

The measures laid down in this Action Plan are designed to bring an immediate and short-term responses to the ongoing threats the EU is facing, notably in the Baltic Sea. The Action Plan sets a holistic approach by addressing the resilience cycle of critical submarine infrastructures. The Commission and the High Representative will engage with Member States and partners, including NATO, to operationalise these actions with a clear objective: to bring concrete solutions to well-defined security challenges.